INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA

2021/2022

TII

CIBERDEFESA E A GESTÃO DO RISCO

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.

Filipa Isabel Carneiro Ferreira Aires

CAP/TOCC

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERDEFESA E A GESTÃO DO RISCO

CAP/TOCC Filipa Isabel Carneiro Ferreira Aires

Trabalho de Investigação Individual CPOS-FA 2021/2022 2.ª Ed.

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERDEFESA E A GESTÃO DO RISCO

CAP/TOCC Filipa Isabel Carneiro Ferreira Aires

Trabalho de Investigação Individual CPOS-FA 2021/2022 2.ª Ed.

Orientador: TCOR/TMMEL Mário Fernando Silvestre Duarte

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Filipa Isabel Carneiro Ferreira Aires**, declaro por minha honra que o documento intitulado **Ciberdefesa e a Gestão do Risco** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial Superior – Força Aérea 2021/2022, 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**, 12** de **julho** de **2022**

Filipa Isabel Carneiro Ferreira Aires
CAP/TOCC

Agradecimentos

Cumprida mais uma etapa da minha carreira militar, quero expressar os mais sinceros agradecimentos a todos aqueles que contribuíram para o sucesso desta missão.

Ao meu orientador, Tenente-Coronel Mário Duarte, pela sua inestimável ajuda, orientação, acompanhamento, disponibilidade, partilha de experiência e recomendações.

Ao diretor de curso e docentes do CPOS FA 21/22 2.ª edição, pelo rumo e preocupação constantes, assim como por todos os conselhos que me deram.

Aos camaradas auditores do CPOS FA 21/22 2.ª edição, pela sã camaradagem e pelos momentos alegres proporcionados.

A todos os entrevistados, que se disponibilizaram para responder às entrevistas.

Aos meus pilares, mãe e marido, pelo apoio incondicional e compreensão que me deram ao longo desta jornada.

Índice

Índice de Figuras

Índice de Quadros

Resumo

A par da evolução tecnológica, as ameaças à segurança das organizações são cada vez mais frequentes, complexas e destrutivas, conduzindo à adoção de medidas defensivas como principal prioridade.

As operações defensivas no ciberespaço consistem em ações que visam preservar a capacidade de utilização do mesmo, a fim de garantir a liberdade de ação, onde o fator segurança é essencial para tratar vulnerabilidades e mitigar impactos com recurso a medidas apropriadas.

Considerando que a edificação da capacidade de ciberdefesa em Portugal, ainda se encontra em processo de consolidação, a presente investigação tem como objetivo avaliar o contributo da gestão do risco para a eficácia da ciberdefesa nas Forças Armadas Portuguesas.

Relativamente ao procedimento metodológico, foi utilizado um raciocínio indutivo, assente na estratégia de investigação qualitativa e no desenho de pesquisa de estudo de caso.

Com a concretização desta investigação, foi possível verificar que, para o processo de gestão do risco ser eficaz, existe a necessidade de utilização de determinadas ferramentas interoperáveis a fim deste processo poder contribuir para melhor perceber o ciberespaço e as ameaças a que estamos expostos, permitindo ainda, perpetrar ações ofensivas no ciberespaço, aferindo a todo o momento eventuais consequências, devido à característica contínua de todas as etapas.

Palavras-chave:

Ameaça, Risco, Ciberespaço, Ciberdefesa, Gestão do Risco, Operações de Ciberdefesa.

Abstract

Alongside technological progress, threats to the security of organisations are increasingly frequent, complex, and destructive, leading to the adoption of defensive measures as the main priority.

Defensive operations in cyberspace consist of actions aimed at preserving the ability to use it safely, where the security factor is essential to address vulnerabilities and mitigate impacts using appropriate measures.

Considering that cyber defence capabilities in Portugal are still in a consolidation process, this research aims to assess the contribution of risk management to the effectiveness of cyber defence in the Portuguese Armed Forces.

Regarding the methodological procedure, inductive reasoning was used, based on a qualitative research method and case study research.

This research verified that, for the risk management process to be effective, certain interoperable tools must be used for this process to contribute to the better understanding of cyberspace and the threats to which we are exposed, and also allowing us to perpetrate offensive actions in cyberspace, while gauging possible consequences, due to the ongoing nature of all stages.

Keywords:

Threat, Risk, Cyberspace, Cyber defence, Risk Management, Cyber defence Operations.

Lista de abreviaturas, siglas e acrónimos

A

AAP	*Allied Administrative Publication*
AJP	*Allied Joint Publication*

C

CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CCDFFAA	Capacidade de Ciberdefesa das Forças Armadas
CCICE	Centro de Comunicações e Informação, Ciberespaço e Espaço
CEM	Conceito Estratégico Militar
CEMFA	Chefe do Estado-Maior da Força Aérea
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CEDN	Conceito Estratégico de Defesa Nacional
CIRC	*Cyber Incident Response Team*
CNCS	Centro Nacional de Cibersegurança
COCIBER	Comando das Operações de Ciberdefesa
CPOS-FA	Curso de Promoção a Oficial Superior da Força Aérea
CSDN	Conselho Superior de Defesa Nacional

D

DCSI	Direção de Comunicações e Sistemas de Informação
DIRCSI	Direção de Comunicações e Sistemas de Informação
DITIC	Direção de Tecnologias de Informação e Comunicações

E

EMA	Estado-Maior da Armada
EMCIBER	Estratégia Militar para o Ciberespaço
EMGFA	Estado-Maior-General das Forças Armadas
EXE	Exército Português

F

FA	Força Aérea Portuguesa
FFAA	Forças Armadas

G

GNS	Gabinete Nacional de Segurança
GR	Gestão do Risco

I

ISO	*International Standardization Organization*
IUM	Instituto Universitário Militar
L	
LDN	Lei da Defesa Nacional
LOBOFA	Lei Orgânica de Base da Organização das Forças Armadas
M	
MAR	Marinha Portuguesa
MDN	Ministério da Defesa Nacional
N	
NATO	*North Atlantic Treaty Organization*
O	
OE	Objetivo Específico
OG	Objetivo Geral
Q	
QC	Questão Central
QD	Questão Derivada
R	
RFA	Regulamento da Força Aérea
S	
SIRESP	Sistema Integrado de Redes de Emergência e Segurança de Portugal
T	
TII	Trabalho de Investigação Individual
U	
UE	União Europeia
V	
VCEME	Vice-Chefe do Estado-Maior do Exército
VCEMFA	Vice-Chefe do Estado-Maior da Força Aérea

1. Introdução

As ameaças à segurança das organizações são cada vez mais frequentes, complexas, destrutivas e coercivas e conduzem à adoção de medidas defensivas como principal prioridade. (NATO, 2021b, p. 1).

Em Portugal, as competências em matéria de cibersegurança estão atribuídas ao Centro Nacional de Cibersegurança[1] (CNCS) e as de ciberdefesa, à área da Defesa Nacional, materializado nas Forças Armadas[2] (FFAA) desde 2019, e mais recentemente concretizada através da publicação da nova Lei Orgânica do Estado-Maior-General das Forças Armadas (LOEMGFA) (Decreto-Lei n.º 19/2022, de 24 de janeiro) onde é definido o Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE) como o órgão para a ciberdefesa cuja finalidade é assegurar "o exercício do comando de operações militares no e através do ciberespaço". (LOEMGFA, DL n.º 19/2022, p. 22).

A gestão do risco (GR) é o processo de identificação, avaliação e controlo do risco decorrente de fatores operacionais a fim de serem tomadas decisões informadas que equilibrem o custo do risco com os benefícios da missão. (NATO, 2021a, p. 113). Uma prática importante na gestão das organizações é a avaliação de riscos de segurança da informação, pois ajuda a identificar, quantificar e priorizar riscos. (Kuzminykh, Ghita, Sokolov e Bakhshi, 2021, p. 602).

A avaliação do risco, como parte integrante do processo da GR numa organização, deverá ser capaz de identificar ameaças, determinar os níveis de risco de segurança cibernética a fim de tomar ações adequadas para um tratamento prioritário de riscos, e ao mesmo tempo, criar uma cultura de risco dentro da organização como processo iterativo que envolva todos os colaboradores alinhando-os com a visão estratégica. (CSA Singapore, 2019, p. 2).

Neste sentido, embora as organizações reconheçam que a avaliação dos riscos é importante para a eficácia da mesma, observam-se ao nível tático algumas questões. Por exemplo, a identificação de riscos orientada à conformidade gerando comportamentos que oferecem uma falsa sensação de segurança, a determinação da probabilidade do risco baseada em tempo e frequência, levando a imprecisões pois nem sempre existe a informação necessária sobre os eventos anteriores, assim como, o tratamento de riscos com controlos e

[1] As competências do CNCS em matéria de cibersegurança estão vertidas no art.º 7.º da Lei n.º 46/2018, de 13 de agosto que estabelece o regime jurídico da segurança do ciberespaço.
[2] As competências das FFAA em matéria de ciberdefesa estão vertidas no ponto 4 do anexo da Resolução do Conselho de Ministros n.º 92/2019 que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

mecanismos de segurança que não abordam totalmente a causa, evidenciando uma fraca articulação dos cenários de risco. (CSA Singapore, 2019, p. 2).

Ao nível estratégico, Nunes (2020, p. 47) no desenvolvimento do trabalho de investigação subordinado ao tema "A edificação da capacidade de ciberdefesa nacional", apresentou como principais contributos nesta área da ciberdefesa, a definição de uma Estratégia Militar para o Ciberespaço (EMCIBER) e o desenvolvimento de uma Capacidade de Ciberdefesa das Forças Armadas (CCDFFAA), cujo objetivo foi preencher um hiato existente entre a articulação da estratégia militar do país e a EMCIBER.

Do ponto de vista operacional, Coelho (2018, p. 29) no seu trabalho intitulado "*O ciberespaço na defesa coletiva e na gestão de crises: a articulação entre a cibersegurança e a ciberdefesa*", baseou-se em casos de diversos países europeus e asiáticos, para afirmar que a relação civil/militar no ciberespaço e as competências de cada um destes atores nesta matéria, não é consensual, pois existem diferentes soluções, muitas delas, baseadas em abordagens experimentais. Refere que existem nações que atribuem as responsabilidades da segurança do ciberespaço à Justiça, outros à Segurança Interna e outros ainda, à Defesa.

Ao nível dos processos, Morgado (2019, p. 34) estudou o nível de *awareness*[3] em Ciberdefesa na Força Aérea Portuguesa (FA), onde concluiu que esse nível é 2 (em desenvolvimento), numa escala de 1 a 5, em que 5 é um nível otimizado. Concluiu também que:

> […] é necessária a constituição de instrumentos que possibilitem o aumento dos conhecimentos, perceção e consciência dos assuntos ligados à ciberdefesa por forma a permitir à Força Aérea atingir níveis mais elevados de *awareness* neste domínio das operações, mitigando o maior número de vulnerabilidades possível, diminuindo consequentemente a exposição ao risco. (Morgado, 2019, p. 34).

Neste sentido, face à inexistência de estudos relativos à GR na ciberdefesa propõe-se desta forma, aferir se a identificação atempada dos riscos cibernéticos e o seu tratamento correto, mitiga o impacto das ameaças atuais sobre a sociedade e em particular sobre as organizações militares.

Considera-se que este trabalho pode acrescentar informação e conhecimento relevante para a consolidação da ciberdefesa e melhor interligação com as demais estruturas da segurança do ciberespaço.

[3] Estado ou condição de estar ciente; ter conhecimento; consciência. *www.dictionary.com*

Neste âmbito, define-se como objeto de estudo a GR enquanto instrumento que permite influenciar a tomada de decisão em matéria de ciberdefesa nas FFAA, delimitando-se nos seguintes domínios (Santos & Lima, 2019):

- Temporal: 12 meses, entre julho de 2021 e junho de 2022;
- Espacial: território nacional;
- Conteúdo: perspetiva organizacional (FFAA).

Estabelece-se como objetivo geral (OG) *avaliar o contributo da gestão do risco para a eficácia da ciberdefesa nas Forças Armadas*, e para o qual irão concorrer os seguintes Objetivos Específicos (OE):

OE1: Caracterizar a gestão do risco e a perceção deste pelas FFAA no âmbito da ciberdefesa.

OE2: Analisar como as FFAA identificam as ameaças à ciberdefesa.

OE3: Avaliar de que forma a gestão do risco influencia a tomada de decisão nas ações de ciberdefesa nas FFAA.

A fim de concretizar os objetivos expressos e dar resposta ao problema de investigação, foi definida a seguinte Questão Central (QC): *De que modo a gestão do risco contribui para a eficácia da ciberdefesa nas FFAA?*

Relativamente à QC, decorreram as seguintes Questões Derivadas (QD):

QD1: Qual o risco no ciberespaço percecionado pelas FFAA no âmbito da ciberdefesa?

QD2: Qual a valorização das ameaças na ciberdefesa?

QD3: Como é que a gestão do risco determina a condução de operações de ciberdefesa nas FFAA?

De forma a alcançar o propósito acima descrito, o presente TII encontra-se organizado em cinco capítulos: no primeiro capítulo é efetuada a introdução ao tema; no segundo capítulo é apresentado o estado da arte através da revisão de literatura, abordando a temática da ciberdefesa, a sua relação com a GR, assim como as fontes de informação e a tipologia de ameaças no âmbito da ciberdefesa e a ligação desta com os diferentes atores; no terceiro capítulo é indicada a metodologia e o método utilizado; no quarto capítulo são apresentados e analisados os resultados obtidos; por fim, no quinto e último capítulo, apresentam-se as conclusões, os contributos para o conhecimento, as limitações e as recomendações para futuras investigações.

2. Enquadramento teórico e concetual

Face à evolução tecnológica observada no âmbito da ciberdefesa ao longo dos últimos anos, surgiram inúmeras abordagens teóricas associadas a esta temática.

Considerando os objetivos da presente investigação, foi decidido recorrer às abordagens teóricas mais consensuais com o modelo de análise da investigação. Neste sentido, no presente capítulo são apresentados contributos teóricos relativos à temática da GR, procurando definir a importância da identificação das vulnerabilidades dos ativos essenciais às FFAA e a forma como todo o processo da GR pode influenciar a tomada de decisão das chefias militares na condução de operações de ciberdefesa nas FFAA.

Este trabalho, insere-se nas Ciências Militares, mais concretamente na área das Técnicas e Tecnologias Militares, incidindo na subárea de ciberdefesa.

2.1. Estado da arte/ revisão de literatura

Para a elaboração do estado da arte, foi dada maior atenção aos conceitos estruturantes desta investigação, tais como a ciberdefesa e a GR. Complementarmente, para melhor se conseguir interligar estes dois conceitos, entendeu-se definir o ambiente onde as operações de ciberdefesa acontecem – o ciberespaço – e o contributo que a cibersegurança tem neste domínio.

Diversas organizações internacionais como a União Europeia (UE) e a *North Atlantic Treaty Organization* (NATO), reconhecem o ciberespaço como novo domínio operacional. Semelhantemente, diferentes autores como Nunes (2020, p. 1), Geraldes (2019, p. 97), Neves (2015, p. 17) e entidades como o *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) (2022, p. 21) e o Ministério da Defesa Nacional (MDN) (Despacho n.º 13692, 2013, p. 31977), consideram que para além dos tradicionais domínios da terra, mar, ar e espaço, o ciberespaço é um novo domínio para as operações.

Os termos ciberespaço, cibersegurança e ciberdefesa são por vezes usados indiferentemente, sendo essa, uma das razões pelas quais estes conceitos muitas vezes se confundem. Neste sentido, a fim de criar uma base concetual sólida, é importante dissipar qualquer incerteza entre estes conceitos, procedendo-se em primeiro lugar ao seu correto enquadramento.

2.1.1 Ciberespaço

É consensual que dados e informação são ideias intrínsecas ao conceito de ciberespaço. Hintzbergen, Hintzbergen, Smulders e Baars (2018, p. 29) observam que “informação é o dado que tem significado”. Os autores mencionam que cada sujeito confere maior ou menor

importância, a determinado conjunto de dados a que tem acesso. Esse acesso é normalmente, feito recorrendo a sistemas de informação, através dos quais, interagem pessoas e dados. Ainda segundo Hintzbergen et al. (2018, p. 31), é nos sistemas de informação, assentes numa determinada infraestrutura, que se dá a transformação dos dados e o respetivo processamento de informação.

O conceito *Data, Information, Knowledge, Wisdom*[4] (DIKW) forma uma Hierarquia de quatro camadas, numa sequência lógica através do qual é possível gerir o conhecimento, conforme se constata na Figura 1. Nela, relacionam-se diferentes estágios, em que a camada posterior abrange a anterior e acrescenta novos atributos. Os dados não possuem significado, fazem parte de um nível mais básico. A informação adiciona contexto aos mesmos. Já o conhecimento é a forma como a informação é utilizada e por último, a sabedoria define quando e por que razão devemos usar o conhecimento que possuímos (Jifa e Lingling, 2014, p. 814).

Figura 1 - Hierarquia DIKW

Fonte: Adaptado a partir de Jifa & Lingling (2014, p. 815)

A utilização da internet e o desenvolvimento das tecnologias criaram novas modalidades de interação entre utilizadores e diferentes formas de trocar informação. O ciberespaço é considerado parte integrante das infraestruturas críticas das sociedades modernas, tendo o seu aparecimento e exploração modificado a maneira como comunicamos e efetuamos trocas de informação (Jayawardane, Larik e Jackson, 2015, p. 3).

Importa compreender que uma rede é um conjunto de sistemas ou objetos ligados entre si e que por essa razão é premente que haja interoperabilidade. O modelo OSI[5] é um modelo que foi criado para normalizar a forma como a informação é transmitida em rede e entre

[4] Dados, Informação, Conhecimento, Sabedoria
[5] OSI – *Open Systems Interconnection*

máquinas. É constituído por 7 camadas em que cada uma delas executa uma determinada função. (Gouveia e Magalhães, 2009, p. 1-5).

A NATO define o ciberespaço como "o domínio global que consiste em todas as comunicações interconectadas, tecnologia e outros sistemas eletrónicos, redes e dados". (NATO, 2020, p. 4)

Identificando que, à semelhança dos restantes domínios (terra, mar, ar, espaço), as atividades da Aliança no ciberespaço, ou através dele, estão expostas a uma ampla gama de ameaças. No entanto, enquanto nos domínios tradicionais, o custo elevado dos meios e capacidades militares para produzir efeitos na guerra balizam as ações no ciberespaço, os recursos de baixo custo podem resultar em efeitos desproporcionais contra a Aliança ou uma nação dependente de tecnologia. (NATO, 2020, p. 6).

A doutrina NATO, define ainda cinco princípios para as operações no ciberespaço: segurança, surpresa, concentração de força, manutenção da moral e a liberdade de ação. Decorrente destes princípios, existem dois tipos de operações no ciberespaço; operações defensivas e operações ofensivas. (NATO, 2020, pp. 15-16).

As operações defensivas consistem em ações que visam preservar a capacidade de utilização do ciberespaço a fim de garantir a liberdade de ação. Inclui avaliação de vulnerabilidades e GR, assim como ações de resposta conforme a necessidade operacional (NATO, 2020, p. 16). Por outro lado, as operações ofensivas podem ser executadas isoladamente ou em conjunto com outras operações. Neste tipo de operação é importante compreender o seu impacto. (NATO, 2020, p. 17).

Dependendo do tipo de operação, ofensiva ou defensiva, assim serão os efeitos produzidos no, ou através do ciberespaço, e ainda nos outros domínios tradicionais das operações. Estes efeitos dividem-se em diretos e indiretos. Os primeiros visam atingir *software*, dados e protocolos. Os segundos, podem visar as outras camadas do ciberespaço, ou até mesmo produzir efeitos nos domínios considerados tradicionais. (NATO, 2020, p. 17).

A interoperabilidade entre sistemas militares, civis, públicos e privados aumenta o risco de efeitos indesejados. Entre outros efeitos, incluem-se os principais: neutralizar, manipular, exfiltrar, degradar, perturbar e destruir. (NATO, 2020, p. 18).

Por seu turno, a UE define ciberespaço como "o conjunto de ativos tangíveis e intangíveis dependentes do tempo, que armazenam e/ou transferem informações eletrónicas" (ENISA, 2017, p. 6).

Em termos nacionais, a Resolução do Conselho de Ministros n.º 36/2015, aprovou pela primeira vez em Portugal, a Estratégia Nacional de Segurança do Ciberespaço (ENSC). Volvidos quatro anos, surgiu a nova ENSC 2019-2023. Esta estratégia define ciberespaço como sendo o "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (ENSC 2019-2023, RCM, 92/2019).

A ENSC 2019-2023 esclarece que as ameaças do ciberespaço se caracterizam:

> "[…] pela sua transversalidade, rápida propagação em rede, anonimização e persistência. Face a esta tipologia de ameaça, apenas uma resposta em rede potenciará e tornará resiliente o esforço […] garantindo um elevado nível comum de segurança do ciberespaço de interesse nacional. (ENSC 2019-2023, RCM n.º 92/2019).

A ENSC tem como propósito definir "objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio". (ENSC, RCM n.º 36/2015)

O CNCS (CNCS, 2022), define ciberespaço como "o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras, por exemplo, através de mensagens eletrónicas, em salas de conversa ou em fóruns de discussão."

2.1.1.1 Cibersegurança

A *European Union Agency for Cybersecurity* (ENISA), Agência Europeia para a Segurança de Redes e da Informação, define cibersegurança como o conjunto das "atividades necessárias para proteger o ciberespaço, seus utilizadores e pessoas afetadas por ameaças cibernéticas". Estas atividades utilizam procedimentos que vão desde a prevenção, passando pela mitigação, até à investigação de incidentes de segurança e considera atributos como autenticidade e não-repúdio para além da disponibilidade, confidencialidade e integridade (ENISA, 2017, p. 6).

Também a doutrina NATO apresenta uma definição de cibersegurança consensual com as anteriormente apresentadas e diz que este conceito resulta da "aplicação de medidas de segurança para a proteção de comunicações, informações e outros sistemas eletrónicos, e que as informações são armazenadas, processadas ou transmitidas nesses sistemas

cumprindo a confidencialidade, integridade, disponibilidade, autenticação e não-repúdio." (NATO, 2020, p. 4).

A ENSC 2019-2023 define cibersegurança como:

> […] o conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem. (ENSC 2019-2023, RCM n.º 92/2019, p. 2889)

De acordo com o CNCS o conceito de cibersegurança é entendido como:

> […] o conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças […] tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação. (CNSC, 2022).

O CNCS é o órgão que contribui para uma "utilização livre, confiável e segura do ciberespaço de interesse nacional" e exerce a função de autoridade nacional em matéria de cibersegurança. Este órgão visa ainda "assegurar o planeamento da utilização não militar do ciberespaço em situação de crise ou de conflito armado, no âmbito do planeamento civil de emergência" (CNCS, 2022).

A fim de "melhorar a capacidade de proteção e de resposta aos desafios do ciberespaço e da segurança da informação", o CNCS define cinco objetivos[6] que compõem "medidas técnicas e processuais, bem como evidências de implementação" que "permitem sistematizar processos, procedimentos e ferramentas […] sendo um importante suporte ao processo de gestão do risco de cibersegurança.". (CNCS, 2019, p. 15 e 46).

2.1.1.2 Ciberdefesa

Segundo a ENSC a "ciberdefesa consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço." (ENSC 2019-2023, RCM, 92/2019, p. 2889).

Diz a Lei da Defesa Nacional (LDN) (Lei Orgânica n.º 3/2021, de 09 de agosto) que as FFAA são a instituição nacional incumbida de assegurar a defesa militar da República. Decorrente da alínea 1 do Art.º 3.º da LOBOFA de 09 de agosto de 2021 "o conceito estratégico militar [...] define as grandes linhas conceptuais de atuação das Forças Armadas e as orientações gerais para a sua preparação, emprego e sustentação.".

[6] Objetivos: Identificar, Proteger, Detetar, Responder e Recuperar.

O Conceito Estratégico de Defesa Nacional (CEDN) (CEDN, RCM n.º 19/2013, 2013) declara que a estratégia nacional se desenvolve em três vetores de ação estratégica, sendo o de "exercício de soberania, neutralização de ameaças e riscos à segurança nacional", aquele onde se enquadra o desenvolvimento de capacidades militares necessárias à mitigação das consequências de ataques cibernéticos.

Por seu turno, o Conceito Estratégico Militar (CEM) aprovado pelo Ministro da Defesa Nacional em 22 de julho de 2014 e confirmado em Conselho Superior de Defesa Nacional (CSDN) de 30 de julho de 2014, declara que "entre as principais ameaças aos Estados [...] destaca-se o ciberterrorismo e os ataques às infraestruturas nacionais de informação e comunicação." e define como sub-cenário de emprego de forças, a ciberdefesa, cuja intervenção das FFAA se cinge à "aplicação de medidas de segurança que garantam a salvaguarda da informação e a proteção das infraestruturas de Comunicações e dos Sistemas de Informação das Forças Armadas contra ciberataques". (CEM, CCEM, 2014)

Nesta linha de pensamento e de ação doutrinária, também a Diretiva Estratégica do Estado-Maior-General das Forças Armadas (EMGFA) 2018-2021 define como um dos seus objetivos estratégicos:

> […] dinamizar a edificação da capacidade de ciberdefesa nacional [...] nos diversos elementos funcionais que constituem uma capacidade operacional [...] aprofundando a colaboração entre o Centro de Ciberdefesa [...] e outros parceiros nacionais e internacionais [...] com o objetivo de dotar as Forças Armadas com capacidade acrescida para defender as redes militares contra ciberataques e realizar operações militares no ciberespaço. (CEMGFA, 2019)

É ainda vertido na LOBOFA (LOBOFA, Lei Orgânica nº. 2/2021), que para os assuntos de ciberdefesa no que ao comando das operações militares no ciberespaço diz respeito, os Chefes de Estado-Maior dos ramos dependem do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA).

De acordo com o explanado no *site* oficial do Ministério da Defesa Nacional, "as atividades de ciberdefesa constituem uma nova área do domínio das operações da Defesa Nacional e um contributo fundamental para a segurança do ciberespaço de interesse nacional." É ainda definido que compete às FFAA as ações de "prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional" (MDN, 2022).

O Centro de Ciberdefesa (CCD), sedeado no EMGFA, é constituído por militares dos três ramos das FFAA (Marinha, Exército e Força Aérea) e garante "a integridade,

confidencialidade e disponibilidade da informação dos sistemas de informação da Defesa Nacional". (MDN, 2022).

De acordo com a Orientação para a Política de Ciberdefesa, os seus objetivos prendem-se com a garantia da proteção, da resiliência e da segurança das redes e dos SIC da Defesa Nacional contra ciberataques, visam "assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional" e contribuem ainda "de forma cooperativa para a cibersegurança nacional.". (MDN, Despacho n.º 13692, 2013, p. 31978).

2.1.2 Gestão do Risco

A GR é o processo de identificação, avaliação e controlo do risco decorrente de fatores operacionais, a fim de serem tomadas decisões informadas que equilibrem o custo do risco com os benefícios da missão. (NATO, 2013, p. 2-R-9). Uma prática importante na gestão das organizações é a avaliação de riscos de segurança da informação, pois ajuda a identificar, quantificar e priorizar riscos. Este subprocesso da GR compreende várias etapas, tais como identificação, gestão, controlo, transferência ou eliminação. (Kuzminykh et al., 2021, p. 602).

2.1.2.1 Risco, ameaça e vulnerabilidade

Primeiramente, risco é definido em função da probabilidade de uma determinada ameaça, aproveitando uma vulnerabilidade num ativo e provocando um impacto resultante dessa ocorrência. Existem muitas definições de risco, no entanto a mais comum é a que o considera como o resultado do impacto que determinada ameaça pode causar. (CSA Singapore, 2019, p. 5). Por outro lado, e de forma mais completa, o risco pode ainda ser definido como a probabilidade de uma determinada vulnerabilidade ser explorada por uma ameaça e que possa causar impacto na organização. (ENISA, 2022, p. 8).

Diz o *Allied Joint Doctrine for Cyberspace Operations*.(AJP 3-20) que a segurança é essencial para a liberdade de ação no ciberespaço, mitigando vulnerabilidades e ameaças com recurso a medidas apropriadas. As ameaças que causam falhas e interrupções de sistemas, podem ser inerentes aos próprios sistemas ou ser causadas por influências externas, sendo que ambas as situações podem ter um impacto disruptivo semelhante. (NATO, 2020, p. 15).

Hintzbergen et al. (2018, p. 37) definem ameaça como "uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização". Por essa razão, Leirvik (2022, p. 139) refere que o nível de maturidade de uma organização pode

aferir-se pela forma como a mesma escolhe medir o risco e mitigar as ameaças. O mesmo autor (2022, p. 161) menciona que o fator tempo utilizado na descoberta das vulnerabilidades, pode ser essencial na seleção das medidas de mitigação.

Vulnerabilidade pode referir-se a uma fraqueza na conceção, implementação e/ou operação de um ativo ou no controlo interno de um processo. O conceito de probabilidade refere-se à possibilidade de que um determinado evento de ameaça seja capaz de explorar uma determinada vulnerabilidade. (CSA Singapore, 2019, p. 5).

Por último, impacto refere-se à "magnitude do dano resultante de um evento de ameaça que explora uma vulnerabilidade". O impacto representa o custo (tangível ou intangível) para a organização (ou em relação ao ativo) que tem de ser suportado se o ataque for realizado com sucesso. Desta forma, as organizações deverão definir qual a sua tolerância ao risco. Determinar a tolerância ao risco permite definir o nível de risco considerado aceitável. (CSA Singapore, 2019, p. 5).

De acordo com a mesma fonte (CSA Singapore, 2019, p. 6), a tolerância ao risco varia entre o nível muito alto, em que o mesmo não pode ser aceite e estratégias de mitigação deverão ser tomadas imediatamente, e o nível baixo, em que o mesmo pode ser aceite, no entanto deverá ser monitorizado periodicamente para garantir que qualquer alteração às circunstâncias é detetada e tratada adequadamente.

De uma forma mais genérica, a avaliação do risco trata da identificação de riscos e determina o nível dos riscos identificados.

Hintzbergen et al. (2018, p. 27) definem avaliação do risco como um "processo geral de identificação do risco, análise do risco e estimativa do risco". Os mesmos autores (2022, p. 32) defendem que o fim último de uma avaliação metódica do risco, conduz a uma ação de gestão adequada às prioridades inicialmente definidas pela organização, levando-a a implementar processos de controlo de riscos apropriados contra as ameaças existentes.

De acordo com o *NATO Security Risk Management Process* (AC/35-D/1035) (NAC, 2005, p. 1-3), a avaliação do risco é um processo de identificação de riscos de segurança, normalmente denominados por ameaças e vulnerabilidades, seguido da determinação do seu impacto e das medidas de controlo necessárias para a salvaguarda da informação dos sistemas. Este tipo de avaliação contribui para uma maior consciencialização de segurança nos vários níveis da organização e não deve cingir-se a um período de tempo específico, mas ser aplicada a todo o momento e de forma periódica a fim de acompanhar as mudanças das ameaças. O sucesso de uma avaliação de risco no âmbito da segurança depende, em grande

parte, do papel dos decisores, na medida em que a gestão de topo de uma organização é o ponto de apoio transversal para que a mesma seja executada em ambiente colaborativo e produza os resultados desejados.

Hintzbergen et al. (2018, p. 43) definem ações de controlo como "salvaguardas ou contramedidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidades devido a ameaças, agindo sobre a sua correspondente vulnerabilidade".

A *International Standard Organization* (ISO) *31000:2018* (ISO, 2018a, p. 3.2) define o processo de GR como um conjunto de "atividades coordenadas para dirigir e controlar uma organização em relação ao risco".

Para implementar o processo de GR numa organização é desejável que a mesma siga uma determinada metodologia. Este conceito é traduzido pela ISO como um conjunto de elementos necessários para colocar em prática o planeamento, a ação, o controlo, revisão e a melhoria de todo o processo de GR (ISO, 2018a).

A metodologia GR utilizada pelas organizações possui fases distintas, uma, em que se avalia o risco no que diz respeito à sua identificação, caracterização e classificação, e outra, que envolve a mitigação e as consequências da exploração das vulnerabilidades. De referir que a estratégia da organização é que define que opções de GR devem ser consideradas. O principal objetivo da GR é a prevenção de ameaças com intuito de reduzir a probabilidade de ocorrência, sendo que as políticas e procedimentos da organização definem a análise de risco-benefício ou custo-benefício. Desta forma, o ideal é encontrar sempre um equilíbrio entre a produção do efeito e o risco associado, através de um processo contínuo de GR. (Piper, 2018, p. 7-5).

De acordo com a ISO/IEC 27005:2018 (2018b, p. 2), *standard* internacional, a GR de segurança da informação deverá ser parte integrante das atividades de gestão das organizações e contribuir para a identificação de riscos e avaliação dos mesmos em função das consequências que poderão causar, assim como, da probabilidade da sua ocorrência. Neste sentido, a GR deverá estabelecer prioridades para o tratamento dos riscos e ainda ser um processo monitorizado frequentemente e revisto regularmente, conforme a Figura 2 que demonstra o Processo de gestão do risco de segurança da informação.

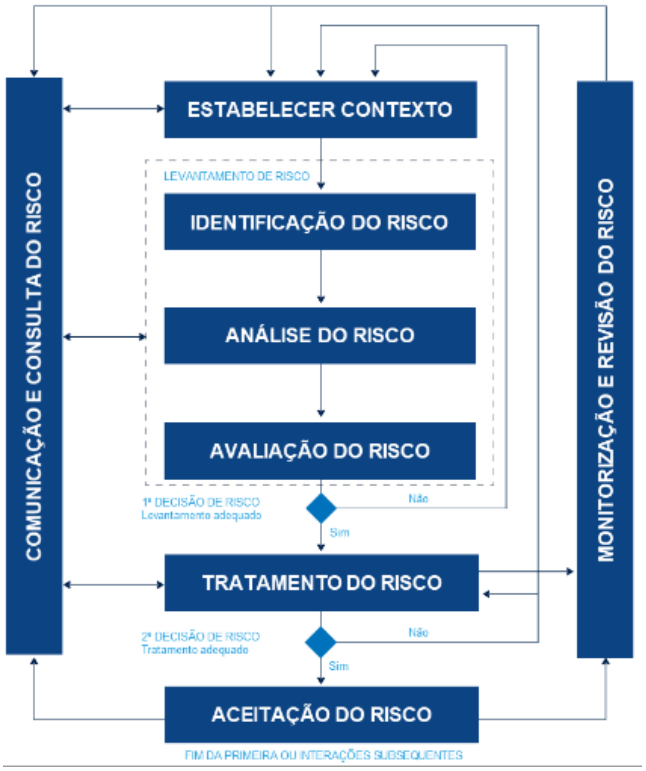

Figura 2 – O processo de gestão do risco de segurança da informação

Fonte: ISO/IEC 27005:2018 (2018b, p. 4).

De acordo com o mesmo manual (2018b, p. 4), este processo cíclico servirá também para decidir se os níveis de risco residual são aceitáveis, e caso não sejam, tratar novamente o risco de forma a mitigá-lo ou, até mesmo, eliminá-lo.

A ISO/IEC 27005:2018 (2018b, p. 17) quando se refere ao tratamento do risco, propõe que as opções disponíveis para tratamento do mesmo, sejam selecionadas com base no resultado, no custo de implementação e nos benefícios esperados. No entanto, "os critérios para a aceitação do risco podem ser mais complexos do que somente a determinação se o risco residual está, ou não, abaixo ou acima de um limite bem definido." Por outro lado, os gestores das organizações devem, também, considerar os riscos improváveis, pois caso se materializem, podem ter impactos gravosos, independentemente do seu tratamento ser menos suportável do ponto de vista económico. (ISO, 2018b, p. 20).

A mesma norma ISO/IEC 27005:2018 (2018b, p. 20), declara que "os riscos não são estáticos. As ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar abruptamente, sem qualquer indicação". De acordo com isto, a monitorização constante é imperativa para que esse tipo de mudança possa ser detetado a tempo e haja uma reação adequada.

Siegel e Sweeney (2020, p. 14) esclarecem que existe um variado número de metodologias *standard* que permitem às organizações utilizar padrões de avaliação apropriados à sua estratégia. Entre elas encontra-se por exemplo a NIST[7], ISACA[8] e ISO/IEC[9].

Siegel e Sweeney (2020, p. 115) afirmam que os controlos podem ser de quatro tipos, definidos em termos das funções que executam, sendo classificados como controlos de dissuasão, prevenção, deteção e correção. São exemplo de controlos de dissuação aqueles que se destinam a desencorajar um potencial invasor, tais como, uma política de segurança robusta ou câmaras de videovigilância. Já os controlos destinados à prevenção visam minimizar a probabilidade de ocorrência de um incidente, como por exemplo, através de controlo de acessos baseados em necessidade de conhecer. Por outro lado, os controlos de deteção, destinam-se a identificar a ocorrência de um incidente, através de alertas do tipo sistema de deteção de intrusos (IDS[10]). Por último, os controlos corretivos destinam-se a corrigir as componentes do sistema após a ocorrência de um incidente, por exemplo através da utilização de *backups* de dados.

O Relatório de Riscos Globais (WEF, 2022, p. 23), publicado pelo *World Economic Forum*, considera que uma das ameaças mais iminentes é a desigualdade digital, visto existirem aproximadamente três bilhões de pessoas sem acesso às tecnologias. No entanto, quanto maior for a interação tecnológica entre os povos, maiores serão as vulnerabilidades associadas a essas ligações. Este relatório conclui, ainda, que as falhas de cibersegurança, continuarão a ser o risco tecnológico com maior gravidade na próxima década.

A rápida evolução tecnológica intensifica os esforços para construir estratégias e produzir doutrina que englobe todos os utilizadores do ciberespaço, nomeadamente, através de iniciativas tecnológicas emergentes como *blockchain*, inteligência artificial e capacidade quântica, a fim de fazer face aos ciberataques (WEF, 2022, p. 53).

A Força Aérea Portuguesa (FA) define o processo de GR como sendo a "sistemática identificação e avaliação de risco, como forma de apoiar e fundamentar a tomada de decisões de risco, e na supervisão da implementação das medidas de controlo" (RFA 25-1(D), 2021, p. 14-4).

[7] *NIST Special Publication 800-30: Guide for Conducting Risk Assessments*
[8] *ISACA Risk Framework – Risk IT*
[9] *The International Organization for Standardization/ International Electrotechnical Commission's (ISO/IEC)*
[10] IDS - *Intrusion Detection System*

Para o Exército Português (EXE) a GR é "um processo que apoia os decisores na tomada de decisão através de uma sistematização na identificação, na avaliação e no controlo do risco resultante de fatores operacionais" no entanto para se tomar essa decisão é crucial "saber se é necessário decidir, quando decidir e o que decidir." (PDE 5-00, 2007, p. E-1).

A Marinha Portuguesa (MAR) entende a GR como:

> […] o processo através do qual as organizações analisam de forma metódica os riscos inerentes às respetivas atividades e processos, bem como os fatores que lhes estão associados, com o objetivo de os identificar, avaliar, controlar e monitorizar, estabelecendo para o efeito as medidas de controlo mais adequadas para […] evitar […] prevenir ou reduzir […] aceitar […] transferir o risco. (IAA 3(C), 2011, p. 5.1).

2.1.2.2 Risco Sistémico

As organizações do setor público, dependem cada vez mais do setor privado, e as infraestruturas críticas de uma nação que utilizam serviços desse setor podem ser afetadas em caso de incidentes cibernéticos, expondo a segurança e resiliência nacional, sendo por isso importante a partilha de informação entre setores. Esta partilha torna-se importante para uma compreensão mais holística do ponto de vista dos riscos transversais e partilhados entre setores para que o impacto seja menor em caso de incidente. Nesta medida, "a partilha de dados fornece informações valiosas sobre a forma como o risco cibernético se manifesta num mundo interconectado e os possíveis danos colaterais que pode causar". (CISA, 2022a).

Identificar ameaças, analisar vulnerabilidades e prever consequências pode ajudar as organizações a desenvolver métricas que afiram a eficácia dos controlos de segurança implementadas, no sentido de conduzir a análises que evitem riscos com maior precisão e confiança. Com estes dados pode entender-se melhor qual "a relação entre ameaça, vulnerabilidade e consequência, para quaisquer funções críticas". (CISA, 2022a). Desta forma, para se compreender o risco é necessário compreender a ameaça.

2.1.3 Atores

Conforme a Figura 3 – Origem das ameaças, Kaffenberger e Kopp (2019, p. 4) admitem que de acordo com o tipo de agente e ameaça, assim variam os recursos para realizar ataques. Por isso é que a GR se afigura como fundamental para ações de ciberdefesa.

	Category	Actions	Real/Possible Impact	Frequency
	**Nation-states**	*Monitor other nations' economies for espionage; conduct cyber-attacks in rare cases.*	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	**Proxy Organizations**	*Steal information for espionage; possibly conduct destructive attacks.*	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	**Cybercrime**	*Steal money from financial sector entities; at times stealing large sums.*	Affects organizations' profits; loss of trust if breach is publicized but org was silent	Theft—very common
	**Hacktivist**	*Disrupt financial sector operations; attack the brand of individual institutions; data release individual/institutions.*	Damaged reputation; loss of trust	Moderately common
	**Insider**	*Steal money; get revenge through destruction or data release.*	Affects organizations' profits; damaged reputation	Moderately rare

Figura 3 - Origem das ameaças

Fonte: (Kaffenberger, L. e Kopp, E., 2019, p. 4)

Os estados-nação focam-se em ações de espionagem e ações ofensivas no ciberespaço, fundamentadas em aspetos geopolíticos e objetivos estratégicos de poder.

Os mesmos autores (Kaffenberger & Kopp, 2019, p. 3) identificam também criminosos, *hacktivistas* e *insiders* como atores suscetíveis de perpetrar ações no ciberespaço que podem causar efeitos nefastos devido ao alto grau de sofisticação que demonstram podendo perturbar gravemente as organizações.

Os atores *proxy* realizam essencialmente ações de espionagem em nome de alguém, como por exemplo, um estado-nação opositor ou um concorrente financeiro, no entanto estas ações ofensivas podem ser fisicamente destrutivas. (Kaffenberger & Kopp, 2019, p. 3).

2.1.4 Eventos, incidentes e quebras de segurança

Evento é um acontecimento (Infopédia, 2022). Significa qualquer ocorrência observável numa rede ou sistema de informação. Considera-se ainda, uma mudança de segurança cibernética que pode ter impacto nas operações organizacionais, incluindo missão, recursos ou reputação (NIST, 2022).

O conceito de ameaça refere-se a qualquer evento, através de um vetor de ameaça, durante o qual o ator responsável pela ação, age contra um ativo com o objetivo de causar danos. Estes eventos caracterizam-se por Táticas, Técnicas e Procedimentos (TTP) (CSA Singapore, 2019, p. 5).

Diversas e, de frequência diária, são as notícias sobre ciberataques em Portugal. Em 08 de fevereiro de 2022, a CNN Portugal divulgou no seu *site* de notícias, alguns dos últimos acontecimentos nesta matéria. O ataque à operadora de telecomunicações Vodafone, ocorrido nesse mesmo dia, apesar de ter causado grande impacto a todos os seus clientes,

não demonstrou indícios de que "os dados de clientes tenham sido acedidos e/ou comprometidos" tendo sido considerado pelo presidente executivo da empresa um «ato criminoso […] com gravidade, para dificultar ao máximo o nível dos serviços» (CNN, 2022). A mesma notícia (CNN, 2022), refere ainda mais ciberataques ocorridos no início do ano, nomeadamente, o ataque aos *sites* da Cofina a 6 de fevereiro de 2022 e o ataque aos diversos *sites* do grupo Impresa a 2 de janeiro do mesmo ano.

Ainda na sequência destas informações, surge a recordação de outros ataques a hospitais (Hospital Garcia de Orta – 2017, Hospital CUF – 2018, Hospital de Ponta Delgada – 2021, Hospital Divino Espírito Santo – 2021), operadoras de comunicações (Altice Portugal – 2020), fornecedores de energia (EDP – 2020) e organismos do Estado (Câmara Municipal de Lisboa – 2017).

Em 27 agosto 2020, o *Diário de Notícias*, relatou no seu *site* que um "ataque informático dirigido a *e-mails* de funcionários" teria parado os "serviços no Ministério da Defesa várias horas". A notícia relatava que o Centro de Ciberdefesa das FFAA teria conseguido impedir a tempo intrusões nos sistemas informáticos e não haveria registo de que tivesse sido exfiltrada informação, no entanto, alguns setores do ministério da Defesa pararam devido a esse ciberataque designado por *Denial-of-Service* (DoS).

Fonte do mesmo órgão de comunicação social (DN, 2022) publicou informação relativa à identificação de ciberataques por parte dos órgãos de Segurança Interna como ameaça a Portugal. Descrevia a notícia que, o CNCS estaria em alerta máximo tendo aumentado o nível de prontidão das suas equipas de resposta contra incidentes informáticos, na sequência do ataque da Rússia à Ucrânia em fevereiro de 2022.

A perspetiva das autoridades policiais e dos serviços de informações é que os ciberataques devem estar no topo das preocupações, não só pelas consequências que este tipo de conflito pode provocar na UE e em parceiros NATO, como também pelo impacto que os ciberataques anteriores provocaram em infraestruturas importantes da sociedade portuguesa, como a Vodafone e o grupo Impresa.

É ainda referido que "outro risco para Portugal […] são os cabos submarinos de comunicações que passam pelo mar nacional, e que são críticos e estratégicos para as ligações entre dezenas de países do continente europeu e americano" e que poderão ser um potencial alvo da Direção-Geral de Pesquisa em Águas Profundas russa pois "uma das suas principais funções é a interceção de comunicações que centenas de cabos submarinos transportam a quilómetros de profundidade, ou até a sua destruição". (DN, 2022)

Em 2018, as FFAA portuguesas terão sido alvo de um ataque informático, no entanto o EMGFA garantiu que:

> […] este ataque foi dirigido à rede de correio eletrónico administrativo utilizado pelos militares e funcionários civis do EMGFA, num total de cerca de 3,5Gb de informação de *emails* exfiltrados […] e que não atingiu, porém, a rede classificada de acesso restrito que funciona paralelamente à rede que foi alvo de intrusão. (Simões, 2019).

Estes exemplos são apenas os mais recentes ocorridos em Portugal, mas que demonstram a importância de um controlo constante em matéria de cibersegurança e consequente ciberdefesa.

2.2. Modelo de análise

Concluída a revisão da literatura é importante compreender qual a perceção das FFAA perante a utilização da GR como contributo relevante na condução de operações de ciberdefesa. Para tal, foram definidas as respetivas dimensões que sustentam o Modelo de Análise, constante no Apêndice A, de modo a alcançar a resposta à problemática.

3. Metodologia e método

Seguidamente, é apresentada a metodologia e o método a utilizar nesta investigação, focando os procedimentos de recolha, classificação, análise e interpretação de dados.

3.1. Metodologia

Pretendeu-se nesta investigação, seguir um raciocínio indutivo. Marconi e Lakatos (2017, p. 93) afirmam que o objetivo fundamental dos argumentos indutivos é o investigador ser conduzido a concluir conteúdos mais vastos que o levem a generalizações, a planos mais abrangentes. Pretendeu-se com este método, observar fenómenos, relacioná-los e construir uma generalização dessas relações.

A abordagem da investigação é do tipo qualitativo em que interpretação dos resultados é feita a partir de padrões encontrados nos dados recolhidos (Vilelas, 2009, p. 105, cit. por Santos & Lima, 2019, p. 27).

No que ao desenho de investigação diz respeito, este trabalho é do tipo estudo de caso. (Santos & Lima, 2019, p. 38).

3.2. Método

Neste subcapítulo são explanados os procedimentos de recolha, classificação, análise e interpretação de dados.

3.2.1. Participantes e procedimento

Participantes. A investigação contou com a colaboração de sete entidades, cinco delas ligadas aos Ramos e EMGFA, denominadas por **E1** a **E5**, e duas individualidades militares, com reconhecidas competências na área, denominadas por **E6** e **E7**, passíveis de acrescentar valor e credibilidade à investigação. As entrevistas foram produzidas com base na análise documental sobre a temática. Os Entrevistados são todos militares, estando a sua identificação esclarecida no Quadro 1.

Quadro 1 - Entrevistados

Código	Órgão/Entidade	Cargo	Titular	Meio de Entrevista	Data da Entrevista
E1	MAR/EMA	Divisão de Redes e Sistemas de Informação – Chefe Ciberdefesa	CFR Câmara de Assunção	*E-mail*	06jun22
E2	MAR/DITIC/NCIRC	Chefe Núcleo CIRC da Marinha	CTEN STP Courela Alexandre	*VTC*	09jun22
E3	EXE/VCEME/DIRCSI	Chefe Departamento de Ciberdefesa e Segurança da Informação	TCOR Paulo Branco	*E-mail*	06jun22
E4	FA/VCEMFA/DIVCSI	Chefe DIVCSI	COR Bruno Cabaço	*Presencial*	09jun22

E5	EMGFA/DIRCSI/CCD	Chefe COpCiberEspaço	TCOR Jorge Vinagreiro	*E-mail*	29jun22
E6	GNS	Diretor-Geral do Gabinete Nacional de Segurança (Autoridade Nacional de Segurança)	CALM António Gameiro Marques	*VTC*	06jun22
E7	SIRESP	Presidente do Conselho de Administração do Sistema Integrado de Redes de Emergência e Segurança de Portugal	BGEN Paulo Viegas Nunes	*E-mail*	08jun22

Procedimento. Relativamente ao procedimento, foram contactadas as entidades a fim de fazer o enquadramento da investigação em causa, solicitando a sua colaboração. Concedido o consentimento, o guião de entrevista estruturada foi enviado por *e-mail* a partir de dia 29 de maio de 2022. A maioria das respostas foi obtida pela mesma via, sendo que outras requereram reunião presencial ou VTC[11]. Em todas as situações, foram acauteladas as questões de anonimato e confidencialidade das respostas, sendo que todos os participantes abdicaram desse facto. As respostas foram devolvidas no período de 06 e 29 de junho de 2022.

3.2.2. Instrumento de recolha de dados

Segundo Sousa e Baptista (2011, cit. por Santos & Lima, 2019), "nas estratégias qualitativas a recolha de dados é efetuada recorrendo à entrevista, à observação e à análise documental". No caso concreto deste trabalho, as técnicas utilizadas foram a análise documental e entrevistas.

Relativamente às entrevistas, estas foram do tipo estruturado onde a abordagem aos assuntos foi previamente determinada e os mesmos convenientemente ordenados. Foi escolhido este tipo de entrevista devido ao facto de o roteiro da mesma ser seguida sem alterações de ordem, forma e conteúdo.

3.2.3. Técnica de tratamento de dados

A fim de efetuar o tratamento qualitativo dos dados recolhidos nas entrevistas estruturadas, recorreu-se à análise de conteúdo. De acordo com Bardin (2011, p. 36) "a análise de conteúdo [...] é um método muito empírico, dependente do tipo de «fala» a que se dedica e do tipo de interpretação que se pretende como objetivo".

Neste caso, a análise de conteúdo foi do tipo categorial, sob a forma de codificação. Foram definidas "categorias, subcategorias, unidades de registo" e unidades de enumeração

[11] VTC – *Video teleconferencing* (videoconferência)

conforme Apêndice E e que foram utilizadas no tratamento das entrevistas de acordo com Apêndice D. (Sarmento, 2013, p. 53).

4. Apresentação dos dados e discussão dos resultados

Neste capítulo são apresentados os dados e discutidos os resultados obtidos com a aplicação do Guião de Entrevista, em Apêndice B, e respondidas as QD e a QC.

4.1. Perceção do risco no ciberespaço pelas FFAA

De acordo com a informação recolhida apurou-se que, face à importância que assume a ciberdefesa e a cibersegurança, os entrevistados consideram que ambas devem estar integradas (E4), pois, quando determinado ciberataque é efetivado e a sua envergadura considerável, é essencial que a ciberdefesa assuma um papel preventivo, antecipando determinadas ações, observando e detetando incidentes, no sentido de promover uma resposta adequada (E1, E6, E7). No que diz respeito a uma ação militar concreta, só o COCiber está autorizado a conduzir esse tipo de operação no ciberespaço (E6, E7).

Os entrevistados consideram que o papel da ciberdefesa perante determinados ataques é definido ao nível da esfera política, e as ações a tomar, definidas em função do evento. É, ainda, um papel colaborativo na medida em que articula partilha de informação das mais diversas fontes sendo o objetivo primordial a salvaguarda do interesse nacional. (E1, E4, E6, E7).

A monitorização e controlo das ameaças deverá ser constante e contínua. Esse controlo deverá ser prioritário de acordo com o tipo de ameaça, e o resultado dessa verificação, partilhado com outras entidades (E2, E3, E5). O principal constrangimento na falta de controlo e monitorização das ameaças reside nos recursos humanos, quer em quantidade, quer em qualificações. (E2, E3, E5).

É através de uma plataforma de gestão conjunta que as demais entidades envolvidas na ciberdefesa contribuem para a determinação do nível de risco no ciberespaço, e onde é depositada informação. O órgão responsável por disponibilizar aos ramos as ferramentas necessárias, é o CCD. Estas ferramentas do tipo *Security Information and Event Management* (SIEM), possibilitam correlacionar eventos, analisar tráfego e gerir incidentes, a fim de concretizar uma resposta atempada (E1, E4, E5, E6, E7).

Para alguns entrevistados, no que diz respeito à prioridade, prevenir e antecipar ameaças é mais importante do que mitigar vulnerabilidades (E2, E3), no entanto, há quem afirme que não deve haver prioridades entre antecipar ameaças ou mitigar vulnerabilidades pois tudo deverá ser considerado prioritário (E5).

4.1.1. Síntese conclusiva e resposta à QD1

Em resposta à QD1, "Qual o risco no ciberespaço percecionado pelas FFAA no âmbito da ciberdefesa", a análise qualitativa das entrevistas permitiu verificar um conjunto de perceções pelas FFAA no âmbito da ciberdefesa relativas ao risco no ciberespaço.

Todos os entrevistados consideram que existe uma boa perceção do risco no ciberespaço pelas FFAA, no entanto as lacunas existentes, essencialmente, com a escassez de recursos humanos, quer em quantidade de efetivo, quer no grau de especialização, juntamente com a perceção de que tudo é prioritário, desde antecipar ameaças a mitigar vulnerabilidades, poderá constituir uma vulnerabilidade podendo, facilmente, levar qualquer organização a perder o momento para responder a um qualquer evento.

4.2. Valorização das ameaças na ciberdefesa

De acordo com a informação recolhida apurou-se que com a entrada em vigor da nova legislação, LDN e LOBOFA, ambas de 2021, a capacidade de ciberdefesa, no que diz respeito ao seu nível de implementação, sofreu algumas alterações orgânicas e de nomenclatura face ao preconizado anteriormente (E1, E4).

O tratamento do risco é da competência dos Ramos e do EMGFA. Na vertente de cibersegurança, é uma responsabilidade de ambos os órgãos, e na vertente das operações de ciberdefesa, é o COCiber que trata os incidentes (E1, E4, E5). As entidades envolvidas neste processo são os Ramos e o EMGFA, sendo que os primeiros apoiam e colaboram (E4) e o EMGFA, através do COCiber, intervém na exploração ofensiva (E1, E5).

Relativamente às ameaças, que se consubstanciam em ataques do tipo *Distributed Denial-of-Service* (DDoS), é referido que acontecem com frequência (E2). Relativamente a ataques à rede elétrica nacional e campanhas de desinformação, afirmam os entrevistados, que essa monitorização é da responsabilidade do CNCS, no entanto, as FFAA reforçam as medidas de segurança com diversos mecanismos a fim de evitar outros constrangimentos. (E2, E3, E5).

Perante determinados eventos, os processos e os procedimentos usados na estrutura de ciberdefesa para tratar o risco, residem na utilização de ferramentas cedidas pelo CCD, *frameworks standard* e alargamento da utilização da autenticação multifator nas diversas plataformas e acessos (E2, E5). No que diz respeito aos procedimentos, as medidas passam por limitar a superfície de ataque, aplicar Técnicas, Táticas e Procedimentos (TTP), normas

internas dos Ramos e outras emanadas pelo CCD ou sugeridas pelo G4[12], conforme a situação em questão (E3, E5, E7).

Identificar atores é difícil, mas estes estão tipificados através de várias fontes de informação (*Intel*) e de análise forense (E2, E3, E5). Por outro lado, a valorização das ameaças é feita pelo CCD e essas instruções transmitidas aos seus subordinados (E2). A responsabilidade desta identificação é atribuída ao CCD, no entanto, não há uma atribuição de ataques a atores, apenas correlações (E3, E5).

Conhecer os ativos e as infraestruturas importantes nas organizações é essencial e confirma-se que existe um bom conhecimento nesta área. (E1, E2, E3, E4, E5). Este nível de conhecimento é fundamental para aferir eventuais vulnerabilidades.

As vulnerabilidades são aferidas com frequência, recorrendo-se a fontes e ferramentas diversas. (E1, E2, E3, E4). Após identificação destas, é comum mitigar as mesmas através da implementação de controlos como por exemplo, a autenticação multifator, ou por tratamento completo, quando possível. (E1, E2).

É entendimento comum que os Ramos participam essencialmente em ações de suporte como, por exemplo, prevenção, deteção e recuperação de incidentes, não desenvolvendo, propriamente, operações no ciberespaço. (E2, E3, E4).

Quando ocorre um incidente, é feito um registo em plataforma própria do tipo IHS (*Incident Handling System*) e que é utilizada exclusivamente no domínio da Defesa (EMGFA, Ramos e MDN) sendo utilizada pelas componentes de ciberdefesa de cada entidade (E1, E2, E3, E4, E5). Há quem conduza análises forenses onde são avaliados os impactos e identificadas evidências (E2, E3, E4, E5) e ainda, delineados planos de resposta com ações de mitigação. (E1, E2, E5). Nas FFAA, a partilha deste tipo de informação é feita através de uma plataforma conjunta onde são depositados todos os dados destes acontecimentos. (E1, E2, E3, E4, E5). É através desta plataforma que as demais entidades envolvidas na ciberdefesa contribuem para a determinação do nível de risco no ciberespaço. (E1, E4, E6, E7).

A doutrina NATO é o principal vetor orientador para a área da ciberdefesa, sendo que os Ramos das FFAA estão alinhados com as práticas emanadas pelo CCD, que, por sua vez, se baseia em doutrina da Aliança. (E1, E4).

[12] G4 – Grupo constituído por CNCS, Serviço de Informações de Segurança (SIS), Polícia Judiciária (PJ) e CCD.

4.2.1. Síntese conclusiva e resposta à QD2

Com base nos dados atrás apresentados, e considerando que a maioria dos entrevistados apresenta respostas tendencialmente alinhadas e coerentes observa-se que em resposta à QD2 "Qual a valorização das ameaças na ciberdefesa", todos os entrevistados consideram que quando ocorre um incidente, a gestão é feita numa plataforma própria que permite a contribuição das FFAA para a determinação do nível de risco no ciberespaço, competindo ao CCD traçar as orientações operacionais para a correção de vulnerabilidades e partilha de informação.

4.3. Influência da gestão do risco na condução de operações de ciberdefesa nas FFAA

De acordo com a informação recolhida apurou-se que as entidades que contribuem para a edificação da capacidade de ciberdefesa no seio das FFAA, ainda que em processo de consolidação, têm uma clara perceção do risco no ciberespaço. (E1, E4, E6, E7).

Os entrevistados consideram que o papel da ciberdefesa perante determinados ataques é definido ao nível da esfera política e as ações a tomar, definidas em função do evento. É, ainda, um papel colaborativo na medida em que a articula a partilha de informação entre as mais diversas fontes sendo o objetivo primordial a salvaguarda do interesse nacional. (E1, E4, E6, E7).

É entendimento comum que os Ramos das FFAA participam essencialmente em ações de suporte como, por exemplo, prevenção, deteção e recuperação de incidentes, não desenvolvendo, propriamente, operações no ciberespaço. (E2, E3, E4).

Os entrevistados consideram que é importante e fundamental implementar um processo de gestão de risco para a realização de ações no ciberespaço. Este processo deverá implementar ações de mitigação e deverá ser contínuo e permanente. (E1, E3, E5, E7).

A avaliação do risco deverá preceder as operações no ciberespaço, e sempre que possível, feita uma avaliação sistémica do mesmo. (E1, E4).

O reporte dos acontecimentos ao escalão superior, relacionados com as ações de ciberdefesa, é realizado através de relatórios específicos e pelos meios à disposição para o efeito, ficando assim o escalão superior envolvido, consciente e atualizado (E4).

Para alguns entrevistados, no que diz respeito à prioridade, prevenir e antecipar ameaças é mais importante do que mitigar vulnerabilidades (E2, E3), no entanto, há quem afirme que não deve haver prioridades entre antecipar ameaças ou mitigar vulnerabilidades pois tudo é considerado prioritário. (E5).

4.3.1. Síntese conclusiva e resposta à QD3

Em resposta à QD3, "Como é que a gestão do risco determina a condução de operações de ciberdefesa nas FFAA?", observa-se ser unânime que a GR deverá orientar a condução de operações de ciberdefesa nas FFAA, baseada numa clara perceção dos riscos no ciberespaço, através do papel colaborativo das entidades envolvidas no processo. A GR deverá ser sempre precedida de uma avaliação das ameaças, para que o escalão superior possa tomar decisões de forma informada. É fundamental implementar um processo de GR de forma contínua, nunca descurando as prioridades em função do cenário a fim de salvaguardar o interesse nacional.

4.4. Contributo da gestão do risco para a eficácia da ciberdefesa nas FFAA e resposta à QC.

O presente estudo foi orientado com o objetivo de obter resposta à questão "De que modo a gestão do risco contribui para a eficácia da ciberdefesa nas Forças Armadas?"

Considerando que as diversas estruturas da ciberdefesa (Ramos e EMGFA) se encontram alinhadas no que concerne aos objetivos a atingir e os resultados a alcançar, é unânime que existe uma perceção do risco existente no ciberespaço pelas FFAA, no entanto, observam-se desde logo algumas vulnerabilidades como sejam a escassez de recursos humanos, que pode condicionar a definição de prioridades, levando uma organização a responder a qualquer evento de forma desproporcional.

Apesar das FFAA estarem cientes da sua exposição às ameaças e da sua valorização ser feita pelo órgão competente, o CCD, é fundamental existirem valências quer no domínio defensivo, para tratar de eventuais vulnerabilidades e evitar a sua exploração por atores com interesses opostos ao interesse nacional, mas também no domínio ofensivo, para antecipar a capacidade de resposta nacional a eventos de larga escala, com elevado risco sistémico.

Neste sentido, verificando que a edificação da capacidade de ciberdefesa nacional está ainda em processo de consolidação, deduz-se que a capacidade existente para desenvolver operações ofensivas no ciberespaço, juntamente com a escassez de recursos humanos, pode conduzir a incidentes mais graves e quebras de segurança no âmbito da defesa nacional.

A GR constitui-se como um processo que permite identificar ameaças e vulnerabilidades ao nível organizacional, de forma transversal. Se conduzido de forma correta poderá não só, orientar a condução de operações de ciberdefesa, mas também, proporcionar um reporte ao escalão superior com maior objetividade e consciência do risco, promovendo a tomada de decisões mais informadas.

Tendo em conta que não existe um processo de GR implementado para as ações de ciberdefesa nas FFAA, observa-se que de forma geral este permitiria melhorar não só a eficácia, mas também a sistematização de processo e procedimentos, a utilização de ferramentas, e o reporte aos decisores no sentido de determinarem ações mais informadas e sustentadas em evidências.

Para tal considera-se importante que a resposta a determinado evento deve ser o mais célere possível e observa-se que a intenção está vertida nos procedimentos utilizados pelas FFAA, demonstrando assim que a estrutura militar tem a ideia, a visão e os mecanismos, no entanto, o processo de GR não está implementado na sua plenitude.

Considera-se que, para o processo de GR existir, deve iniciar-se de raiz, com procedimentos bem definidos onde subsista um efetivo levantamento das ameaças e dos ativos críticos, sejam implementados controlos, se proceda à avaliação e análise dos riscos e por último o seu tratamento eficaz. Desta forma, considera-se que a GR deverá ser um processo holístico, que permite orientar e levar as organizações a tomar melhores decisões no tratamento e resolução de eventos perante determinados cenários.

Em suma, a GR contribui para perceber melhor o ciberespaço e a sua envolvência, ajudando a compreender o que nos rodeia, designadamente os atores e as ameaças.

5. Conclusões

A par da evolução tecnológica, as ameaças à segurança das organizações são cada vez mais frequentes, complexas, destrutivas e coercivas conduzindo à adoção de medidas defensivas como principal prioridade.

Decorrente desta evolução, surgem novos domínios das operações militares e observa-se que o ambiente operacional tem vindo a sofrer alterações quer na forma como as operações são conduzidas, quer nos efeitos que produzem.

Considerando que em Portugal, as competências em matéria de cibersegurança estão atribuídas ao CNCS e as de ciberdefesa, à área da Defesa Nacional, materializado nas Forças Armadas, pretendeu-se demonstrar com a presente investigação, a existência de uma relação entre os conceitos de ciberdefesa e de GR numa perspetiva que permita às diferentes entidades militares uma tomada de decisão mais informada e priorizada, garantindo continuidade das operações em segurança.

Atendendo ao novo domínio das operações, o ciberespaço já é considerado parte integrante das infraestruturas críticas das sociedades modernas, tendo o seu aparecimento e exploração, alterado a maneira como comunicamos. A utilização da internet e o desenvolvimento das tecnologias criaram novas modalidades de interação entre utilizadores e diferentes formas de trocar informação.

Não obstante as FFAA apresentarem um conjunto de normativos legais e o emprego de boas práticas, a complexidade do ciberespaço transporta em simultâneo uma tipologia de ameaça, que apenas uma resposta em rede garante um elevado nível comum de segurança de interesse nacional.

Neste sentido, a presente investigação teve como objeto de estudo a GR enquanto instrumento que permite melhorar a tomada de decisão em matéria de ciberdefesa nas FFAA, encontrando-se delimitada nos seguintes domínios: temporal, últimos 12 meses (entre julho de 2021 e junho de 2022); espacial, em território nacional e de conteúdo à perspetiva organizacional, no sentido de compreender a influência da gestão dos riscos cibernéticos na tomada de decisão das ações de ciberdefesa nas FFAA.

Relativamente ao procedimento metodológico, foi utilizado um raciocínio indutivo, assente numa estratégia de investigação qualitativa e no desenho de pesquisa de estudo de caso.

Foram estabelecidos três OE, que concorrem para o OG e direcionam a investigação. Como OE1, “Caracterizar a gestão do risco e a perceção deste pelas FFAA no âmbito da

ciberdefesa", com base nas entrevistas realizadas foi possível apurar que existe uma boa perceção do risco do ciberespaço pelas FFAA, no entanto, verificam-se lacunas tecnológicas e humanas. As FFAA têm a clara perceção do risco no ciberespaço, mas a escassez de recursos humanos, quer em quantidade, quer em qualificações, associada à desigualdade digital, apresenta-se como uma das ameaças mais iminentes. Percecionar claramente o risco antecipa ameaças e mitiga vulnerabilidades.

No que concerne ao OE2, "Analisar como as FFAA identificam as ameaças à ciberdefesa", verifica-se que que as FFAA estão conscientes da sua exposição às ameaças e que a categorização das mesmas é feita pela pelo CCD. Esta ação constitui um processo que permite corrigir vulnerabilidades, quando a partilha de informação entre os diversos intervenientes é eficaz. Esta partilha no âmbito da ciberdefesa, sendo exclusiva do domínio da Defesa (EMGFA, Ramos e MDN), permite alcançar uma reação mais rápida para apoiar qualquer dos intervenientes.

Relativamente ao OE3, "Avaliar de que forma a gestão do risco influencia a tomada de decisão nas ações de ciberdefesa nas FFAA", foi possível apurar que a GR é fundamental para orientar a condução de operações de ciberdefesa nas FFAA de forma contínua, nunca descurando as prioridades em função do cenário a fim de salvaguardar o interesse nacional e para que o escalão superior possa tomar decisões mais informadas, baseadas essencialmente numa clara perceção dos riscos no ciberespaço.

No que concerne ao OG "Avaliar o contributo da gestão do risco para a eficácia das ciberdefesa nas FFAA", verifica-se que a GR é uma componente importante e com intervenção direta nas ações de ciberdefesa, uma vez que aquilo que se decidir tem impacto na salvaguarda dos interesses nacionais, tornado esta área responsável por contribuir para a segurança dos sistemas em utilização nas FFAA.

Como contributo para o conhecimento emerge da análise efetuada a necessidade de implementação de um modelo transversal de GR nas FFAA de forma a tornar mais eficazes as ações no âmbito das operações de ciberdefesa.

Relativamente às limitações identifica-se que o conhecimento desta matéria é muito limitado a um determinado número de entidades existente nas FFAA e que, apesar dos esforços, ainda existe um longo caminho a percorrer, essencialmente em matéria de especialização na área da ciberdefesa e GR.

No que diz respeito a estudos futuros, recomenda-se a realização de uma investigação sobre qual o modelo de GR para a ciberdefesa que pode ser implementada pelas FFAA, no

sentido de efetivar-se o preconizado na legislação mais recente.

Relativamente a recomendações de ordem prática, sugere-se:

- a implementação de processos de GR na área da ciberdefesa;
- a implementação de incentivos que contribuam para a retenção e contratação de talentos a fim de consolidar a robustez da capacidade de ciberdefesa nacional.

Em jeito de conclusão, o que não se vê, tende a não existir, sendo que desta forma podemos não detetar as vulnerabilidades existentes.

Referências bibliográficas

Bardin, L. (2011). *Análise de Conteúdo. Edição Revista e Ampliada.* Edições 70. Retirado de https://bunker2.zlibcdn.com/dtoken/c8625c33137973e4793c5de24700cd52

Cable News Network (CNN). (2022, 8 fevereiro). *Ciberataques: cronologia de outros ataques em Portugal além da Vodafone.* [Página *online*]. Retirado de https://cnnportugal.iol.pt/mario-vaz/ataque-informatico/vodafone-e-a-mais-recente-vitima-em-seis-anos-de-ciberataques/20500208/62028bd00cf21847f0a9ddfa

Centro Nacional de Cibersegurança (2019). *Quadro Nacional de Referência para a Cibersegurança*. Retirado de https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

Centro Nacional de Cibersegurança (2021). *Relatório Cibersegurança em Portugal: Políticas Públicas.* Retirado de https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriocibersegurança-cncs.pdf

Centro Nacional de Cibersegurança (2022, 7 de maio). [*Página online*]. Retirado de https://www.cncs.gov.pt/pt/sobre-nos/#oquee

Chefe do Estado-Maior-General das Forças Armadas. (2019). *Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2018-2021.* Versão 2. 31 de outubro de 2019. Lisboa: Autor.

Coelho, J. (2018). *O ciberespaço na defesa coletiva e na gestão de crises: a articulação entre a cibersegurança e a ciberdefesa*. Editora: IUM. Retirado de https://comum.rcaap.pt/bitstream/10400.26/24522/1/TII_CMG_SCoelho.pdf

Conselho de Chefes de Estado-Maior (2014). *Conceito Estratégico Militar.* Lisboa: Conselho de Chefes de Estado-Maior

Cooperative Cyber Defence Centre of Excellence. (2022, 7 de maio). [Página *online*]. Retirado de https://ccdcoe.org/about-us/

Cybersecurity & Infrastructure Security Agency (CISA). (2022a, 30 de abril). [Página *online*]. *Systemic Cyber Risk Reduction.* Retirado de https://www.cisa.gov/systemic-cyber-risk-reduction

Cybersecurity & Infrastructure Security Agency (CISA). (2022b, 30 de abril). [Página *online*]. *Cyber threat source descriptions.* Retirado de https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions

Cyber Security Agency of Singapore (CSA Singapore). (2019). *Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure* – Retirado de https://www.csa.gov.sg/-

/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf

Decreto-Lei n.º 19/2022, de 24 de janeiro (2022). *Estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas*. Diário da República n.º 16/2022, 1ª Série, 16, 3 a 97. Lisboa: Presidência do Conselho de Ministros. Retirado de https://data.dre.pt/eli/dec-lei/19/2022/01/24/p/dre/pt/html

European Union Agency for Cybersecurity (ENISA). (2017). *Overview of cybersecurity and related terminology – Version 1*. Retirado de https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

Estado-Maior do Exército (2007). *PDE 5-00 - Planeamento Táctico e Tomada de Decisão.* Lisboa: Autor.

Estado-Maior da Força Aérea, Inspeção-Geral da Força Aérea. (2021). *RFA 25-1 (D) - Sistema de Inspeção da Força Aérea.* Lisboa: Autor.

Geraldes, S. (2019). *A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou Otimista?* Instituto Universitário de Lisboa (ISCTE-IUL), Centro de Estudos Internacionais. Revista Nação e Defesa. Dezembro 2019. N.º 154 pp. 91-108.

Gouveia, J., Magalhães, A. (2009). *Redes de Computadores - Curso Completo. 7.ª Edição Revista e Atualizada.* Editora: FCA - Editora de Informática

Hintzbergen, J., Hintzbergen, K., Smulders, A., Baars, H. (2018). *Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002.* (3ª edição revista). (A. Sá, Trad.). Hertogenbosch: Van Haren Publishing. Retirado de https://pt.pt1lib.org/book/11013549/12e1d9

Inspeção-Geral da Marinha. (2011). *IAA 3 (C) – Atividades de Inspeção*. Lisboa: Autor.

International Organization for Standardization (2018a). *ISO 31000:2018 (en) Risk management — Guidelines.* Retirado de https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

International Organization for Standardization (2018b). *ISO/IEC 27005:2018 (en). Risk technology – Security techniques – Information security risk management.* Retirado de https://swab.zlibcdn.com/dtoken/c5ef3511a2b8e6176cb1fbe0ae31b362

Jayawardane, S., Larik, J., e Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance.* Policy Brief 17. The Hague,

Netherlands. Retirado de https://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf

Jifaa, G., Linglingb, Z. (2014). *Data, DIKW, Big data and Data science.* 2nd International Conference on Information Technology and Quantitative Management, ITQM. Retirado de www.sciencedirect.com.

Kaffenberger, L. e Kopp, E. (2019) *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment.* Carnegie Endowment for International Peace. Publications Department. Washington, DC. Retirado de https://carnegieendowment. org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). *Information Security Risk Assessment.* Encyclopedia, 1(3), 602–617. Disponível em https://doi.org/10.3390/encyclopedia1030050

Lei Orgânica n.º 2/2021, de 9 de agosto (2021). *Aprova a Lei Orgânica de Bases da Organização das Forças Armadas, revogando a Lei Orgânica n.º 1 -A/2009, de 7 de julho*. Diário da República, 1.ª Série, 153, 2 a 17. Lisboa: Assembleia da República. Retirado de https://files.dre.pt/1s/2021/08/15300/0000200017.pdf

Lei Orgânica n.º 3/2021, de 9 de agosto (2021). *Altera a Lei de Defesa Nacional, aprovada pela Lei Orgânica n.º 1 -B/2009, de 7 de julho*. Diário da República, 1.ª Série, 153, 18 a 36. Lisboa: Assembleia da República. Retirado de https://dre.pt/dre/legislacao-consolidada/declaracao-rectificacao/2009-67356360

Leirvik, R. (2022). *Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program*. Arlington: Apress. Disponível em https://doi.org/10.1007/978-1-4842-7821-5

Marcelino, V. (2020, 27 de agosto). *Ciberataque parou serviços no Ministério da Defesa várias horas.* [Página *online*]. Retirado de https://www.dn.pt/pais/ciberataque-parou-servicos-no-ministerio-da-defesa-varias-horas-12558174.html

Marcelino, V. (2022, 26 fevereiro). *Segurança Interna identifica ciberataques como maior ameaça a Portugal.* [Página *online*]. Retirado de https://www.dn.pt/sociedade/seguranca-interna-identifica-ciberataques-como-maior-ameaca-a-portugal-14627854.html

Marconi, M., Lakatos, M. (2017). *Fundamentos da metodologia científica.* 8.ª ed. São Paulo: Atlas. Retirado de https://pt.pt1lib.org/book/5458485/ba3194

Ministério da Defesa Nacional (2013). *Despacho n.º 13692/2013. Orientação Política para a Ciberdefesa.* Lisboa. Retirado de Diário da República, 2.ª série — N.º 208 — 28 de outubro de 2013.

Ministério da Defesa Nacional (2022, 07 de junho). [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

Morgado, P. (2019). *Nível de awareness em ciberdefesa na Força Aérea Portuguesa*. Editora: IUM. Retirado de https://comum.rcaap.pt/bitstream/10400.26/30004/1/TII%20CAP%20PEDRO%20MORGADO.pdf

National Institute of Standards and Technology (NIST) (2022, 7 de junho). [Página *online*]. *Computer Security Resource Center - Glossary*. Retirado de https://csrc.nist.gov/glossary/term/event

Neves, P. (2015). *Capacidade de resposta a incidentes de segurança da informação no ciberespaço - Uma abordagem DOTMLPI-I.* Dissertação para a obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço. Mestrado em Segurança da Informação e Direito no Ciberespaço. Instituto Superior Técnico.

North Atlantic Council (2005). AC/35-D/1035. *NATO Security Risk Management Process (NSRMP).* NATO Security Committee. Bruxelas: Autor.

North Atlantic Treaty Organization. (2020) *Allied Joint Publication 3.20 - Allied Joint Doctrine for Cyberspace Operations*. NATO Standardization Office. Bruxelas: Autor.

North Atlantic Treaty Organization. (2021a). *Allied Administrative Publication-06 – NATO Glossary of Terms and Definitions (English and French)* (Ed. 2021). Bruxelas: Autor.

North Atlantic Treaty Organization (2021b). *NATO Cyber Defence.* Factsheet. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

Nunes, P. (2020). *Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Edificação de uma Estratégia Militar para o Ciberespaço*. Coleção "Ares", 36. Lisboa: Instituto Universitário Militar.

Piper, J. (2018). STO-MP-IST-166 *Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis.* STO - Meeting Proceedings Paper. Retirado de https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-166/MP-IST-166-07.pdf

Porto Editora – evento no Dicionário infopédia da Língua Portuguesa [em linha]. Porto: Porto Editora. [consultado em 27 de junho de 2002]. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/evento

Resolução do Conselho de Ministros n. º 19/2013, de 21 de março (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981 a 1995. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho (2015). *Aprova a Estratégia Nacional de Segurança do Ciberespaço.* Diário da República, 1.ª Série, 113, 3738 a 3742. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 92/2019, de 05 de junho (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.* Diário da República, 1ª Série, 108, 2888 a 2895. Lisboa: Presidência do Conselho de Ministros.

Santos, L. A., & Lima, J. M. (2019). *Orientações metodológicas para elaboração de trabalhos de investigação.* Lisboa: (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2013) *Metodologia científica para a elaboração, escrita e apresentação de teses*. Colecção: Manuais. Local: Lisboa. ISBN: 978-989-640-143-6.

Siegel, C., Sweeney, M. (2020). *Cyber Strategy Risk-Driven Security and Resiliency.* Boca Raton: Auerbach Publications. [versão PDF]. Retirado de https://pt.pt1lib.org/book/5645222/fa3042

Simões, S. (2019, 17 de abril). *Forças Armadas foram alvo de um ataque informático.* [Página *online*]. Retirado de https://observador.pt/2019/04/17/forcas-armadas-foram-alvo-de-um-ataque-informatico/

World Economic Forum (2022). *The Global Risks Report 2022.* 17th Edition. Marsh McLennan, SK Group and Zurich Insurance Group. Retirado de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Apêndice A — Modelo de Análise

Objetivo Geral	Avaliar o contributo da gestão do risco para a eficácia da ciberdefesa nas Forças Armadas				
Questão Central	De que modo a gestão do risco contribui para a eficácia da ciberdefesa nas Forças Armadas?				
Objetivos Específicos	**Questões Derivadas**	**Conceitos**	**Dimensões**	**Indicadores**	**Recolha de Dados**
OE1 – Caracterizar a gestão do risco e a perceção deste pelas FFAA no âmbito da ciberdefesa.	**QD1 –** Qual o risco no ciberespaço percecionado pelas FFAA no âmbito da ciberdefesa?	**Risco** **Ciberespaço** **Ciberdefesa**	Humana Tecnológica	Evidências documentais Respostas das Entrevistas	Entrevistas estruturadas Análise documental
OE2 – Analisar como as FFAA identificam as ameaças à ciberdefesa.	**QD2 –** Qual a valorização das ameaças na ciberdefesa?	**Ameaça** **Atores**	Estratégica Operacional Tática	Evidências documentais Respostas das Entrevistas	Entrevistas estruturadas Análise documental
OE3 – Avaliar de que forma a gestão do risco influencia a tomada de decisão nas ações de ciberdefesa nas FFAA	**QD3 –** Como é que a gestão do risco determina a condução de operações de ciberdefesa nas FFAA?	**Gestão do Risco** **Operações de ciberdefesa**		Evidências documentais Respostas das Entrevistas	Entrevistas estruturadas Análise documental

Apêndice B — Guião de Entrevista Estruturada

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA
2021/2022 – 2.ª EDIÇÃO

ENTREVISTA ESTRUTURADA

A presente entrevista insere-se no âmbito do Trabalho de Investigação Individual (TII) da CAP/TOCC Filipa Isabel Carneiro Ferreira Aires, a frequentar o Curso de Promoção a Oficial Superior da Força Aérea 2021/22 2.ª Edição, no Instituto Universitário Militar, intitulado "Ciberdefesa e a Gestão do Risco". Esta investigação tem por objetivo avaliar o contributo da gestão do risco (GR) para a eficácia da ciberdefesa nas Forças Armadas.

Durante o processo da GR, as organizações deverão ser capazes de identificar ameaças e determinar os níveis de risco de segurança cibernética a fim de tomar ações adequadas para um tratamento prioritário dos mesmos e, ao mesmo tempo, criar uma cultura de risco dentro da organização como processo iterativo que envolva e alinhe todos os colaboradores com a visão estratégica.

Atendendo que atualmente existe alguma capacidade de ciberdefesa instalada, no que se refere a recursos humanos, infraestruturas e recursos materiais, e que subsiste uma necessidade de implementá-la na plenitude, surge a necessidade de, através deste TII, se demonstrar a relação entre os conceitos de ciberdefesa e GR numa perspetiva que permita às organizações uma tomada de decisão de forma informada e priorizada, garantindo para tal a confidencialidade, disponibilidade e integridade da informação e consequente continuidade das operações.

Considerando que este trabalho pode acrescentar informação e conhecimento relevante para a consolidação da ciberdefesa e melhor interligação com as demais estruturas da segurança do ciberespaço, o contributo de V. Exa. é muito relevante para o sucesso desta investigação e, por conseguinte, irá enriquecer o conteúdo deste trabalho.

Pelo referido, e assumindo que todos os dados recolhidos visam apenas a investigação científica, solicito autorização para que as suas respostas, ou extratos das mesmas, devidamente contextualizados, sejam citados e identificados. Se, todavia, não desejar ser identificado ou pretender não responder a determinada pergunta, serão salvaguardadas as garantias de **confidencialidade** e **anonimato**.

Muito grata pela sua colaboração!
CAP TOCC Filipa Aires

Guião da Entrevista Estruturada ao Ex^{mo} Sr. [nome do entrevistado]

Data:
Hora (Local):
Suporte: *e-mail / VTC / presencial*
Posto:
Especialidade:
Nome:
Função:

Pergunta 1: Com a entrada em vigor das novas LDN e LOBOFA, ambas de 2021, qual o nível de implementação da capacidade de ciberdefesa? Que entidades nacionais colaboram/participam no processo de integração da capacidade de ciberdefesa? Como estão divididas as diferentes responsabilidades de cada entidade? A quem compete tratar o risco?
Pergunta 2: A edificação da capacidade de ciberdefesa no seio das FFAA, ainda está em processo de consolidação. Comparando o nosso percurso com outros Países e organizações de que Portugal faz parte (NATO e UE), considera que a capacidade de ciberdefesa nacional já possui uma perceção do risco existente no ciberespaço? A atual noção de risco integra a cibersegurança e a ciberdefesa? Como são discriminados os riscos de ciberdefesa, comparativamente aos de cibersegurança?
Pergunta 3: Conforme noticiado nos órgãos de comunicação social, Portugal tem sido alvo de ciberataques nas mais diversas áreas da sociedade, incluindo na estrutura das FFAA (MDN, EMGFA, etc.). Perante estes acontecimentos, quais os processos e procedimentos usados pela estrutura de ciberdefesa para tratar os riscos?
Pergunta 4: Em junho de 2017, a Ucrânia foi alvo de um ciberataque (*Malware NotPetya*) que infetou computadores de bancos, ministérios, empresas ucranianas, espalhando-se por outras organizações internacionais com escritórios no país, incluindo instituições globais nos setores de transporte marítimo. Qual o papel da ciberdefesa num evento desta envergadura?
Pergunta 5: No âmbito da ciberdefesa, como são atualmente identificados os atores e valorizadas as ameaças? A quem compete tal responsabilidade?
Pergunta 6: As principais ameaças que se encontram a ser monitorizadas pela ciberdefesa incluem a proliferação de DDoS, ataques à rede elétrica nacional e desinformação? Que outras mais?
Pergunta 7: Considera que a sua organização tem conhecimento suficiente sobre os seus ativos e sobre as suas infraestruturas mais importantes? O atual nível de conhecimento permite aferir vulnerabilidades, implementar controlos de segurança e desenvolver operações no ciberespaço? Que tipo de operações no ciberespaço é a sua organização capaz de desenvolver?
Pergunta 8: Na sua organização existe uma monitorização constante das ameaças a que estamos expostos, ou apenas é realizado um registo isolado de eventos/ incidentes de nível Elevado e Crítico? Julga existirem ameaças ou vulnerabilidades, no âmbito de ciberdefesa que não estão a ser tratadas pela sua organização, mas que deveriam? Quais?
Pergunta 9: Qual o contributo da sua organização para a determinação do nível de risco percecionado pela ciberdefesa?
Pergunta 10: Quando ocorre um incidente na sua organização, é produzido algum relatório no âmbito da ciberdefesa? Em caso afirmativo, esse relatório inclui uma avaliação da ameaça ou vulnerabilidade e correspondente estratégia de tratamento do risco? Como flui esta informação dentro da sua organização? Como é feita a comunicação com as demais entidades?
Pergunta 11: Considera existir envolvimento do escalão superior da sua organização na avaliação dos riscos de ciberdefesa? Se sim, de que forma e como é informado o escalão superior?
Pergunta 12: A sua organização cumpre com os requisitos mínimos em termos de ciberdefesa definidos pela NATO [AC/322-D(2017)0047]? Se não, quais os referenciais seguidos pela sua organização na implementação de controlos ou mecanismos de segurança no âmbito da ciberdefesa?
Pergunta 13: Como avalia a necessidade de implementar um processo gestão do risco específico para a realização de ações no ciberespaço?
Pergunta 14: A condução de operações no ciberespaço deverá ser precedida de uma avaliação do risco? A avaliação do risco deve, sempre que possível, ter em conta uma aferição sistémica do risco?
Pergunta 15: Como profissional na área da ciberdefesa, o que considera prioritário: antecipar as ameaças ou mitigar vulnerabilidades?

Apêndice C — Questões da Entrevista por QD e nível

	Questão Derivada			Orgão			
Nº	QD1	QD2	QD3	Divisão de EM	Direção Técnica	Núcleo CIRC	**Pergunta**
P1		x		x			Com a entrada em vigor das novas LDN e LOBOFA, ambas de 2021, qual o nível de implementação da capacidade de ciberdefesa? Que entidades nacionais colaboram/participam no processo de integração da capacidade de ciberdefesa? Como estão divididas as diferentes responsabilidades de cada entidade? A quem compete tratar o risco?
P2			x	x			A edificação da capacidade de ciberdefesa no seio das FFAA, ainda está em processo de consolidação. Comparando o nosso percurso com outros Países e organizações de que Portugal faz parte (NATO e UE), considera que a capacidade de ciberdefesa nacional já possui uma perceção do risco existente no ciberespaço? A atual noção de risco integra a cibersegurança e a ciberdefesa? Como são discriminados os riscos de ciberdefesa, comparativamente aos de cibersegurança?
P3		x			x	x	Conforme noticiado nos órgãos de comunicação social, Portugal tem sido alvo de ciberataques nas mais diversas áreas da sociedade, incluindo na estrutura das FFAA (MDN, EMGFA, etc.). Perante estes acontecimentos, quais os processos e procedimentos usados pela estrutura de ciberdefesa para tratar os riscos?
P4	x	x	x	x			Em junho de 2017, a Ucrânia foi alvo de um ciberataque (*Malware NotPetya*) que infetou computadores de bancos, ministérios, empresas ucranianas, espalhando-se por outras organizações internacionais com escritórios no país, incluindo instituições globais nos setores de transporte marítimo. Qual o papel da ciberdefesa num evento desta envergadura?
P5		x			x	x	No âmbito da ciberdefesa, como são atualmente identificados os atores e valorizadas as ameaças? A quem compete tal responsabilidade?
P6	x	x				x	As principais ameaças que se encontram a ser monitorizadas pela ciberdefesa incluem a proliferação de DDOS, ataques à rede elétrica nacional e desinformação? Que outras mais?
P7		x	x	x	x	x	Considera que a sua organização tem conhecimento suficiente sobre os seus ativos e sobre as suas infraestruturas mais importantes? O atual nível de conhecimento permite aferir vulnerabilidades, implementar controlos de segurança e desenvolver operações no ciberespaço? Que tipo de operações no ciberespaço é a sua organização capaz de desenvolver?
P8	x	x	x		x	x	Na sua organização existe uma monitorização constante das ameaças a que estamos expostos, ou apenas é realizado um registo isolado de eventos/ incidentes de nível Elevado e Crítico? Julga existirem ameaças ou vulnerabilidades, no âmbito de ciberdefesa que não estão a ser tratadas pela sua organização, mas que deveriam? Quais?
P9	x	x	x	x			Qual o contributo da sua organização para a determinação do nível de risco percecionado pela ciberdefesa?
P10		x	x	x	x	x	Quando ocorre um incidente na sua organização, é produzido algum relatório no âmbito da ciberdefesa? Em caso afirmativo, esse relatório inclui uma avaliação da ameaça ou vulnerabilidade e correspondente estratégia de tratamento do risco? Como flui esta informação dentro da sua organização? Como é feita a comunicação com as demais entidades?
P11		x	x	x	x		Considera existir envolvimento do escalão superior da sua organização na avaliação dos riscos de ciberdefesa? Se sim, de que forma e como é informado o escalão superior?
P12		x		x	x		A sua organização cumpre com os requisitos mínimos em termos de ciberdefesa definidos pela NATO [AC/322-D(2017)0047]? Se não, quais os referenciais seguidos pela sua organização na implementação de controlos ou mecanismos de segurança no âmbito da ciberdefesa?
P13			x	x	x		Como avalia a necessidade de implementar um processo gestão do risco específico para a realização de ações no ciberespaço?
P14		x	x	x	x		A condução de operações no ciberespaço deverá ser precedida de uma avaliação do risco? A avaliação do risco deve, sempre que possível, ter em conta uma aferição sistémica do risco?
P15	x	x	x		x	x	Como profissional na área da ciberdefesa, o que considera prioritário: antecipar as ameaças ou mitigar vulnerabilidades?

Apêndice D — Matriz de Análise de Conteúdo das Entrevistas Estruturadas – Unidades de Contexto e Registo

Entrevistado	Unidade de Contexto	Unidade de Registo
Q1 - Com a entrada em vigor das novas LDN e LOBOFA, ambas de 2021, qual o nível de implementação da capacidade de ciberdefesa? Que entidades nacionais colaboram/participam no processo de integração da capacidade de ciberdefesa? Como estão divididas as diferentes responsabilidades de cada entidade? A quem compete tratar o risco?		
E1	O diploma que traz algumas alterações em termos orgânicos à capacidade de ciberdefesa	1.1
	Face ao pouco tempo que estes diplomas têm, não seria expectável que se observassem grandes evoluções no nível de implementação da capacidade	1.2
	As entidades que integram a capacidade de ciberdefesa são o EMGFA, com o COCiber, e os Ramos, com as suas componentes de ciberdefesa	1.1
	Compete ao COCiber (…) propor, planear, coordenar e conduzir operações militares no e através do ciberespaço em apoio a objetivos militares e na salvaguarda da soberania nacional	1.3
	as componentes de ciberdefesa dos Ramos sob a autoridade técnica e funcional deste órgão (COCiber)	1.4
	A responsabilidade na exploração pró-ativa do ciberespaço em prol da condução de operações com objetivos militares está confinada ao COCiber, só o comando de operações de Ciberdefesa é que se encontra autorizado a desenvolver operações de resposta, exploração e ofensivas no ciberespaço	1.3
	Os Ramos têm responsabilidade nas operações mais relacionadas com a cibersegurança das suas infraestruturas, nomeadamente na prevenção e resposta a incidentes	1.4
	o risco a que as Forças Armadas estão sujeitas em termos de ataques informáticos (…) Este risco deve ser tratado ao nível do Ramo uma vez que são os Ramos que conhecem a sua infraestrutura e os seus utilizadores	1.4
	o risco inerente à realização de operações no, e através do, ciberespaço que visem a produção de efeitos (…) esta avaliação é da responsabilidade do EMGFA/COCiber	1.5
E4	O nível de implementação da capacidade de ciberdefesa é a mesma, tal como já se encontrava preconizado nas versões anteriores destes diplomas	1.2
	para os Ramos, estas novas versões trazem algumas alterações e que especificamente a LOBOFA, vem clarificar algumas questões	1.1
	LOEMGFA implementa algumas alterações de nomenclatura e ainda alguns ajustes em termos orgânicos à capacidade de ciberdefesa	1.1
	não se observam grandes alterações no nível de implementação da capacidade face ao que já havia anteriormente	1.1
	Quanto ao tratamento do risco, é função do EMGFA este desiderato, pois é a entidade que tem orçamento, material e recursos humanos	1.4
	os Ramos por estarem sob a autoridade técnica e funcional deste órgão, apoiam-no, essencialmente através da estrutura dos CIRC.	1.2
	a Força Aérea está alinhada com as restantes estruturas de ciberdefesa nacional.	1.1
Q2 - A edificação da capacidade de ciberdefesa no seio das FFAA, ainda está em processo de consolidação. Comparando o nosso percurso com outros Países e organizações de que Portugal faz parte (NATO e UE), considera que a capacidade de ciberdefesa nacional já possui uma perceção do risco existente no ciberespaço? A atual noção de risco integra a cibersegurança e a ciberdefesa? Como são discriminados os riscos de ciberdefesa, comparativamente aos de cibersegurança?		
E1	ainda não se conseguiu chegar aos níveis que se considerem satisfatórios no que respeita à avaliação e tratamento do risco inerente a este domínio das operações	2.1
	são percecionados pela generalidade da comunidade os riscos inerentes ao ciberespaço	2.1
	em riscos inerentes às atividades de prevenção, proteção e defesa das redes e sistemas de informação das FFAA (cibersegurança)	2.1
	riscos resultantes da condução de operações militares no ciberespaço pelas FFAA (ciberdefesa)	2.1

	No que respeita aos segundos (ciberdefesa), uma vez que o COCiber ainda não desenvolve operações para a produção de efeitos no ciberespaço, ainda não existe qualquer doutrina neste sentido, embora considere que esta análise deva estar alinhada com a análise de risco efetuada no âmbito da produção de efeitos nos restantes domínios de operações (mar, terra e ar).	2.3
E4	Sim, a capacidade de ciberdefesa nacional possui uma perceção do risco existente no ciberespaço. Posso afirmar que a perceção existe, mas a materialização do plano de ação passa essencialmente pelo volume de orçamento e disponibilidade de recursos humanos.	2.1
	Quanto à noção de risco de cibersegurança e ciberdefesa, posso dizer que ambas se encontram integradas e que as entidades envolvidas no processo de avaliação das ameaças comunicam entre si e partilham essa informação.	2.2
E6	considero que sim, no entanto, perceção do risco é uma coisa, consubstanciar essa perceção em ações concretas é outra.	2.1
	existe uma lacuna, porque uma estratégia pressupõe um plano de ação que vai endereçar riscos e que, de facto, consubstancia a estratégia, isto é, transforma a estratégia em iniciativas, sendo essas iniciativas priorizadas em função dos riscos.	2.1
	Considero que a capacidade atual de ciberdefesa está assente no desenvolvimento de doutrina, na criação de competências nas pessoas	2.1
	esta estrutura tem sido alvo de investimento em termos de material juntamente com outras iniciativas no sentido de fazer recrutamento de pessoas adequadas para as funções, no entanto estou em crer que pouco foi feito na área das operações de ciberespaço propriamente dito, ainda que não esteja ao corrente dos detalhes do processo.	2.1
	parece-me que neste momento, ainda temos um longo caminho a percorrer, incluindo a área da formação mesmo com a existência da "Academia de Ciberdefesa". Todo este investimento vai levar algum tempo até termos retorno.	2.1
	considero que os riscos são conhecidos, mas considero existir ainda um gap entre a edificação da capacidade e a capacidade existente no nosso país para fazer face a esses riscos	2.1
	Esse risco, para ser mitigado depende exclusivamente de nós, da nossa capacidade que é relativamente baixa em ter talento nessa área, reter esse talento e formar esse talento.	2.1
	considero que existe uma razoável perceção do risco, por parte de uma pequena parte da sociedade, no entanto o risco maior não é o do ciberespaço, é o da nossa própria realidade social, dado que temos ainda uma baixa literacia digital.	2.1
	considero que sim, mas antes de haver uma perceção e uma consequente ação mitigadora desse risco existente no ciberespaço, é preciso endereçar outros problemas, e que por muito que compreendamos o risco existente no ciberespaço se não for endereçado para edificar essa capacidade, sobretudo na dimensão humana, não chegamos lá	2.1
E7	tem sido marcado por alguns constrangimentos, essencialmente ao nível do vetor de capacidade "pessoal".	2.1
	A escassez de recursos humanos tem sido um fator condicionador do processo de edificação desta capacidade limitando a consecução do nível de ambição definido	2.1
	Apesar de existir um alinhamento doutrinário com a NATO e com a EU, revelador de uma boa perceção do risco existente no ciberespaço	2.1
Q3 - Conforme noticiado nos órgãos de comunicação social, Portugal tem sido alvo de ciberataques nas mais diversas áreas da sociedade, incluindo na estrutura das FFAA (MDN, EMGFA, etc.). Perante estes acontecimentos, quais os processos e procedimentos usados pela estrutura de ciberdefesa para tratar os riscos?		
E2	as medidas que a Marinha tomou foram no sentido de limitar a superfície de ataque, isto é, "fechou portas" que pudessem representar vulnerabilidades	3.2 / 3.1
	implementação de autenticação multifator no acesso aos portais da organização que exigem autenticação, assim como nos acessos VPN (Virtual Private Network).	3.1
	fazemos mais análise de vulnerabilidades do que análise de risco, aplicando controlos para mitigar essas vulnerabilidades	3.1
	análise de risco deve ser efetuada de acordo com uma framework que envolva a organização como um todo	3.1
	na Marinha, podemos dizer que se aproxima mais à framework NIST (The NIST Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover), do National Institute of Standards and Technology	3.1
	lacunas em todo este processo, essencialmente por falta de recursos humanos com skills em cibersegurança e gestão do risco, assim como atribuição de recursos financeiros para este fim, em consonância com algumas barreiras que são levantadas à aplicação do risco.	2.1

E3	Relativamente ao Exército, os procedimentos adotados em casos de ameaças que se traduzem em incidentes de segurança, estão tipificados em normas internas emanadas pela Autoridade Técnica (DCSI) e também pela entidade coordenadora nacional, o Centro de Ciberdefesa.	3.2
	Cada Ramo aplica as TTPs (Técnicas, Táticas e Procedimentos) mais adequadas de acordo com o nível de ameaça e gestão do risco aplicado aos sistemas CSI afetados.	3.2
E5	A gestão do risco é uma componente que deverá estar presente em todo o ciclo de vida de uma infraestrutura tecnológica	3.2
	Centro de Ciberdefesa suporta uma infraestrutura tecnológica que disponibiliza aos ramos as ferramentas necessárias para monitorizar e identificar possíveis ameaças e poder agir atempadamente. Estas ferramentas vão desde um sistema de correlação e eventos (SIEM), Análise de tráfego, gestão de incidentes e ainda uma plataforma a que designamos de gestão do risco que por si só não designa o Risco abordado neste tema, mas garantidamente contribui para ele.	3.1 / 2.1
	O que esta plataforma faz é análise de vulnerabilidades aos sistemas em produção nas FFAA e consoante as vulnerabilidades detetadas, atribui um nível de risco dos sistemas afetados.	3.2
	o Centro de Ciberdefesa poderá, com base na componente de CyberThreat Intel, emanar diretrizes no sentido de se reduzir o risco associado a determinado tipo de atores ou existência de vulnerabilidades críticas.	3.2
	a existência de equipas de reação rápida para apoiar os ramos é fundamental para que, na iminência ou após um ataque, este seja resolvido o mais rapidamente possível.	3.1 / 3.2
E6	De facto, Portugal está sujeito a ataques no seu ciberespaço de interesse nacional, como qualquer outro Estado que esteja ligada à Internet	2.1
	Não considero que sejam ameaças de ciberdefesa, são ameaças à segurança do ciberespaço de interesse nacional que depois se consubstanciam em ciberameaças.	2.1
	eu caracterizaria as ameaças pela origem, isto é, pelo tipo de atores que as perpetram.	5.1
	A origem das ameaças está relativamente bem caracterizada	5.1
	o propósito desses ataques é que poderá diferir em função do contexto, sendo que o propósito determina o tipo de informação que desejam obter, e, portanto, os alvos que pretendem atacar e assim os efeitos que pretendem produzir.	5.1
	Portugal está exposto a esses riscos, em função dos seus interesses, das alianças e das estruturas onde está inserido e da forma como se alinha com os seus parceiros e os seus aliados.	2.1
E7	De forma a articular a capacidade de cibersegurança e ciberdefesa nacional (...) foi criado um grupo de coordenação informal, designado por Grupo dos 4 (CNCS, SIS, PJ e Centro de Ciberdefesa das FFAA).	3.2
	Face à tipologia dos ataques, ao seu impacto, à sua natureza e ao nível do risco daí decorrente, a resposta operacional será coordenada ao nível do G4.	3.2
Q4 - Em junho de 2017, a Ucrânia foi alvo de um ciberataque (Malware NotPetya) que infetou computadores de bancos, ministérios, empresas ucranianas, espalhando-se por outras organizações internacionais com escritórios no país, incluindo instituições globais nos setores de transporte marítimo. Qual o papel da ciberdefesa num evento desta envergadura?		
E1	prevenção do seu acontecimento dentro do universo das redes da Defesa Nacional.	4.1
	capacidade militar que, neste caso, atuará exclusivamente na esfera da cibersegurança, ou seja, na prevenção, deteção e resposta a incidentes nas redes da Defesa Nacional	4.1 / 4.2 / 4.3
	ótica colaborativa com as restantes entidades nacionais e internacionais, por forma a minimizar os impactos deste tipo de ataques	4.5
E4	Depende do que superiormente for definido, mais concretamente na esfera política	4.5
	A ciberdefesa terá a intervenção necessária em função do tipo de evento e a forma como esse estiver categorizado, isto é, a intervenção será tanto maior, quanto maior for a ameaça à soberania nacional e assim estiver definido.	4.5
E6	nesse contexto, a ciberdefesa poderia ter ajudado, na dimensão de antecipação, por exemplo através da componente de inteligence.	4.1
	o CNCS, na componente de observação, também o faz, observa, orienta, decide e age, no entanto não pode agir através de Computer Network Operations. Nós, GNS/CNCS, não podemos fazer Computer Network Operations, mas coordenamos a resposta a incidentes de cibersegurança a fim de repor o estado inicial, numa lógica de resiliência.	4.2 / 4.3

	o Comando das Operações de Ciberdefesa (COCiber), se mandatado pelo Governo para tal, tem legitimidade para fazer Computer Network Operations em todas as suas dimensões, exploração das fragilidades do outro, espionagem no espaço do outro, inteligence gathering, e até mesmo, ataque, isto é, lançar armas cibernéticas no espaço do outro.	4.4
	Neste caso concreto, a ciberdefesa poderia ter ajudado através dos seus canais de informação	4.5
	Se um ataque daquela natureza acontecesse hoje, em Portugal, estou convencido que as organizações já estariam mais capacitadas para fazer face a essa situação porque temos mais anos de experiência e temos passado por algumas situações semelhantes.	4.3
	neste momento, investimos muito mais em capacitação, em material e já existem políticas públicas que enquadram esse tipo de acontecimentos, como por exemplo a Lei n.º 46/2018 de 13 de agosto e o Decreto-Lei n.º 65/2021 de 30 de julho, que enquadram os procedimentos necessários a uma ação concreta neste âmbito.	4.3
	É evidente que a tecnologia pode mitigar esses riscos, mas não consegue mitigá-los todos.	4.5
E7	Desta forma, à ciberdefesa compete fazer face a ameaças externas e a situações em que esteja em causa a salvaguarda dos interesses e da soberania nacional	4.5
	competirá às Forças Armadas atuar, nomeadamente através da condução de operações no ciberespaço, destinadas a assegurar a ciberdefesa do País	4.4
	Se acontecesse uma situação desta natureza (ataque a uma infraestrutura crítica), competiria à organização atacada, através do seu Security Operations Center (SOC) assegurar a resposta de 1ª linha, procurando repor a situação	4.3 / 4.5
	será ativada a intervenção das Forças Armadas que, supletivamente e como último recurso, procurarão eliminar o ataque, utilizando para esse efeito operações defensivas e ofensivas no ciberespaço, socorrendo-se, se necessário e como último recurso, do apoio do NCIRC NATO.	4.4
Q5 - No âmbito da ciberdefesa, como são atualmente identificados os atores e valorizadas as ameaças? A quem compete tal responsabilidade?		
E2	As ameaças são identificadas através de várias fontes (intelligence), tais como Centro Nacional de Cibersegurança (CNCS), Centro de Ciberdefesa (CCD), Serviço de Informações de Segurança (SIS), NATO Computer Incident Response Capability (NCIRC) e fontes Open Source de Intel.	5.1 / 5.2
	muitas vezes o CCD define o nível de ameaça, dá indicações e quem recebe essas indicações, atua em conformidade no sentido de mitigar as vulnerabilidades	5.2
	Marinha já trabalha com plataformas de análise, nomeadamente na cloud, através das plataformas Microsoft Security Center – Threat Analysis e Microsoft Defender (EDR).	5.1
	normalmente a ameaça está associada a uma vulnerabilidade	5.1
	Esse valor obtém-se através da fórmula R=PAxI (Risco = Probabilidade da Ameaça x Impacto).	5.1
E3	Os atores não são identificados de forma tradicional, pois o ciberespaço não tem fronteiras e a capacidade de anonimização é elevada	5.1
	Hoje em dia é extremamente difícil identificar os atores maliciosos, sendo necessário um nível de análise forense complexa	5.1
	É aceite pela comunidade com responsabilidades na segurança do ciberespaço em geral que o nível de ameaça mais elevado tem origem num tipo de atores caracterizado como APTs (Advanced Persistent Threat),	5.2
	A responsabilidade de identificar os atores não pertence a nenhum organismo específico, mas sim a quem conduz as operações de análise forense e de análise da atividade suspeita em redes e sistemas.	5.3
	No caso das Forças Armadas, o Centro de Ciberdefesa tem assumido um papel bastante importante nesta área.	5.4
E5	Os atores estão tipificados e o CCD possui uma plataforma que atualiza de forma automática através de conetores externos a organizações de Cyber Intel e de forma manual de acordo com as ligações de Intel que possuímos, nomeadamente internas (CISMIL), externas nacionais (SIS, PJ e CNCS, o denominado G4) e externas internacionais como é o caso da NATO, EU e outras organizações e países com os quais existem acordos de cooperação.	5.1 / 5.3
	Atualmente não fazemos atribuição de ataques a atores, mas conduzimos todo o processo para associar estes atores a incidentes ocorridos nas FFAA e isto é feito através do conhecimento que temos dos atores, nomeadamente as suas TTP's, ferramentas, código utilizado e fontes de informação.	5.3
Q6 - As principais ameaças que se encontram a ser monitorizadas pela ciberdefesa incluem a proliferação de DDOS, ataques à rede elétrica nacional e desinformação? Que outras mais?		

E2	Ataques do tipo DDoD (distributed denial-of-service) acontecem com alguma frequência, embora existam outro tipo de ataques constantes, como por exemplo, ataques a Web Servers que recorrem a diversas técnicas entre elas command injection over http, brute force…etc	6.1 / 6.4
	foram reforçadas medidas, nomeadamente através da implementação de MFA (multi factor authentication) em todos os sites.	6.4
E3	no caso do Exército, existem mecanismos de monitorização e deteção de diversas ameaças	6.4
	Quanto à questão da rede elétrica nacional e campanhas de desinformação não compete ao Exército esta análise, pois a responsabilidade primária nesta área está sob a alçada do Centro Nacional de Cibersegurança (CNCS)	6.2 / 6.3
E5	Estas ameaças que descreve às infraestruturas críticas ou prestadores de serviços essenciais não são da responsabilidade e não são monitorizados pela Ciberdefesa mas sim pelo Centro Nacional de Cibersegurança.	6.2 / 6.4
	A Ciberdefesa foca-se exclusivamente em conduzir operações no Ciberespaço e pela Cibersegurança dos sistemas CSI das FFAA.	6.4/2.2/.3
Q7 - Considera que a sua organização tem conhecimento suficiente sobre os seus ativos e sobre as suas infraestruturas mais importantes? O atual nível de conhecimento permite aferir vulnerabilidades, implementar controlos de segurança e desenvolver operações no ciberespaço? Que tipo de operações no ciberespaço é a sua organização capaz de desenvolver?		
E1	a Marinha tem o conhecimento dos seus ativos mais importantes e maior valor operacional	7.1
	efetua análises de vulnerabilidades com frequência a estes sistemas e, quando necessário, procede à correção das vulnerabilidades	7.2 / 7.4
	A Marinha, na sua componente de ciberdefesa, atua basicamente na componente de cibersegurança, ou seja na prevenção, deteção e recuperação de ciber incidentes, podendo ainda efetuar análise forense a sistemas que tenham sido alvos de ataques.	7.5
E2	É muito importante conhecer aquilo que temos, para que possamos proteger, e para proteger é preciso identificar	7.1
	Este tipo de identificação deve ser visto como um todo	7.5
	A gestão de ativos é um processo em edificação. A Marinha utiliza a plataforma da Microsoft System Center Configuration Manager (SCCM) para inventário, o Security Center na Cloud que permite visibilidade geral e o Solar winds para a gestão de ativos (routers e switches).	7.1
	Relativamente aos ativos críticos, estes são identificados de acordo com a sua função	7.1
	um ativo do tipo firewall de perímetro é um ativo crítico tendo em conta que é a primeira barreira de proteção	7.1
	os servidores de serviços, também são considerados ativos críticos.	
	Os ativos críticos são assim definidos em função do impacto que a sua inoperatividade pode causar à organização, ou seja tendo em conta o seu value.	7.1
	No que diz respeito à identificação de vulnerabilidades, esta pode vir de diferentes fontes, entre as quais o CCD e o Security Center. Existem outras ferramentas como o Acunetix e Nessus para aferir scans de vulnerabilidades.	7.2
	No que aos controlos de segurança diz respeito, utilizamos o MFA no acesso à VPN	7.3
	Marinha apenas atua na componente de suporte, não executando operações ofensivas. Dentro da cibersegurança apenas fazemos Vulnerability Assessement, Security Remediation e Cyber Forensics.	7.5
E3	O Exército tem todo o conhecimento necessário para proteger os seus ativos	7.1
	conhecimento extenso e profundo de todos os sistemas e redes em produção nas suas infraestruturas.	7.1
	Existem atualmente em produção mecanismos automáticos e manuais que permitem aferir com frequência o nível de vulnerabilidades existentes e ativar medidas de proteção e mitigação	7.2
	De acordo com a doutrina NATO de referência (AJP-3.20 , Allied Joint Doctrine for Cyberspace Operations) todos os aliados devem ser capazes de operar no ciberespaço ao nível da defesa e proteção dos seus ativos mantendo a capacidade de operar livremente no, e, através do ciberespaço.	7.5
	O Exército encontra-se alinhado com a doutrina NATO e Nacional nestas matérias.	7.5
E4	Considero que a Força Aérea tem o conhecimento dos seus ativos mais importantes e de maior valor operacional.	7.1
	Todos os dias a Força Aérea afere vulnerabilidades nos sistemas.	7.2

E5	A nossa organização, por si só, já tem incutida uma determinada cultura de segurança, muito provavelmente oriunda do nosso ADN militar, no entanto se não houver investimento em formação, torna-se difícil acompanhar o desenvolvimento tecnológico.	7.5
	Relativamente às operações no ciberespaço, a Força Aérea, na sua componente de ciberdefesa, atua essencialmente na componente de cibersegurança, na prevenção, deteção e recuperação de ciber incidentes.	7.5
	O EMGFA e as FFAA têm pessoas competentes e o conhecimento da infraestrutura, contudo o problema é que as pessoas são poucas e o conhecimento e as capacidades técnicas são adquiridos ao longo do tempo.	7.1
	a gestão de pessoal nas FFAA apresenta-se ineficaz nestas áreas, fruto da elevada mobilidade dos militares e os condicionalismos da carreira militar, o conhecimento muitas vezes perde-se e as capacidades adquiridas não se passam.	7.5
Q8 - Na sua organização existe uma monitorização constante das ameaças a que estamos expostos, ou apenas é realizado um registo isolado de eventos/ incidentes de nível Elevado e Crítico? Julga existirem ameaças ou vulnerabilidades, no âmbito de ciberdefesa que não estão a ser tratadas pela sua organização, mas que deveriam? Quais?		
E2	Existe na Marinha uma monitorização constante a eventos e flows, através da plataforma SIEM, provenientes de várias fontes	8.1
	Uma ameaça está associada a um risco e existem vários modos de responder ao risco, nomeadamente aceitar o risco, transferir o risco, partilhar o risco, remover o risco ou mitigar o risco	8.2 / 8.3
	não se consegue reduzir o risco associado a uma ameaça a zero.	8.1
	Um dos grandes problemas nas organizações é indubitavelmente o fator humano	8.4
	A falta de consciência para a cibersegurança dos recursos humanos é uma vulnerabilidade. Formação constante para consciencializar os utilizadores, é uma das soluções.	8.4
E3	O Exército efetua uma monitorização constante e continua de todos os eventos considerados relevantes para a segurança das suas redes e sistemas	8.1/.2/.3
	Estes eventos são categorizados de acordo com o nível de ameaça e gestão do risco afeto aos ativos.	8.2 / 8.3
	Todos os eventos que originaram um incidente ou considerados como um potencial incidente de segurança, de acordo com a Taxonomia Nacional de classificação de incidentes de Cibersegurança, da NATO e também da EU, em vigor, são registados e mantidos por tempo suficiente para garantir a aplicação da lei, se necessário	8.2 / 8.3
	Todas as novas vulnerabilidades detetadas na RDE são tratadas com prioridade elevada, independentemente do sistema em causa, sendo aplicados mecanismos corretivos para eliminar ou mitigar essas vulnerabilidades	8.2 / 8.3
E5	Os processos implementados no centro de Ciberdefesa determinam que todo o conhecimento Intel é criado e registado numa plataforma para o efeito e toda a informação existente é partilhada no domínio de Defesa (Que inclui também o MDN).	8.2
	As ameaças ou vulnerabilidades que existem referem-se aos problemas sistémicos da falta de pessoal qualificado e alguma deficiência no processo de tratamento do risco na fase do projeto e consequentemente na operação dos sistemas CSI.	8.4
Q9 - Qual o contributo da sua organização para a determinação do nível de risco percecionado pela ciberdefesa?		
E1	Marinha contribui para esta perceção garantindo a realização das análise e correção de vulnerabilidades nos sistemas de informação e comunicação, ficando os resultados destas análises integrados numa plataforma de gestão comum ao EMGFA e Ramos	9.1
E4	A Força Aérea, na sua componente de ciberdefesa, tem um relacionamento diário de partilha constante de informação com o CCD através de plataformas próprias para o efeito.	9.1
E6	o Centro Nacional de Cibersegurança funciona na estrutura do Gabinete (GNS), portanto, o Centro é que contribui na prática para isso, no âmbito da cultura de gestão de riscos	9.1
	nas Forças Armadas, temos uma cultura muito mais orientada ao risco	9.1
E7	Uma vez que esta consubstancia uma rede dedicada com redundância de meios, a SIRESP tem vindo a servir como backup às organizações nacionais que desempenham funções-chave na resposta a emergências e situações de crise nacional, nomeadamente, em caso de ocorrência de um ciberataque disruptivo.	9.1
Q10 - Quando ocorre um incidente na sua organização, é produzido algum relatório no âmbito da ciberdefesa? Em caso afirmativo, esse relatório inclui uma avaliação da ameaça ou vulnerabilidade e correspondente estratégia de tratamento do risco? Como flui esta informação dentro da sua organização? Como é feita a comunicação com as demais entidades?		

E1	Sim (…) é efetuado um relatório com base nas medidas de mitigação do incidente	10.1
	reportando as medidas que foram implementadas para fazer face às vulnerabilidades exploradas e desta feita atuar preventivamente para a ocorrência de novos incidentes	10.3/ 10.2/ 10.4
	incidentes dentro das FFAA são partilhados com o COCiber através da plataforma conjunta de gestão de resposta a incidentes	10.6
	Toda a comunicação é efetuada, internamente, com recurso às plataformas de gestão, bem como recorrendo a sistemas de informação mais informais como sejam o correio eletrónico e plataformas de Chat	10.5
E2	Quando surge um incidente na Marinha (...) é criado um incidente numa plataforma de registos de incidentes transversal aos Ramos e CCD. De seguida, é implementado um plano de resposta (ICTIC4 – Contenção na resposta a um incidente de cibersegurança).	10.1/ 10.6/ 10.4
	Durante o processo de análise forense é elaborado relatório com todas as evidências identificadas e reportado ao CCD.	10.1 a 10.6
	o contacto com entidades públicas é efetuado via CCD/CNCS.	10.6
E3	O Exército, através da sua Autoridade Técnica, reporta todos os incidentes pelo canal determinado para o efeito, neste caso, para o Centro de Ciberdefesa do EMGFA	10.1/ 10.6
	Todos os relatórios de incidente têm por base uma análise macro da ameaça, sistemas afetados, e potencias vetores de ataque que possam colocar em risco os outros Ramos e até o próprio EMGFA,	10.2/ 10.3
	Os mecanismos para troca de informação estão superiormente determinados, e que incluem plataformas e redes especificas.	10.1
E4	esse facto é comunicado e partilhado.	10.1/ 10.6
	Dependendo da ameaça, e caso o evento se revista de maior gravidade, é efetuado um estudo mais aprofundado e uma análise mais detalhada por parte do CIRC.	10.2/ 10.3
	é partilhado baseado na necessidade de conhecer (Need-to-Know) através de plataformas conjuntas de gestão para estes casos.	10.6
E5	todo o registo é efetuado na plataforma para o efeito (IHS – Incident Handling System) onde todas as atividades efetuadas no âmbito da investigação até à conclusão do incidente, são registadas.	10.1
	Esta plataforma é comum aos ramos e quando é do interesse, os incidentes são partilhados.	10.6
	No caso de incidentes com nível de severidade mais elevada, é elaborado um relatório que descreve o incidente e propõem medidas de mitigação e por vezes recomendações.	10.1 a 10.4
	Estes relatórios, conforme o tipo de incidente, são submetidos para despacho superior e são distribuídos de acordo com a necessidade de saber das entidades interessadas.	10.5 e 10.6
Q11 - Considera existir envolvimento do escalão superior da sua organização na avaliação dos riscos de ciberdefesa? Se sim, de que forma e como é informado o escalão superior?		
E1	*Não respondeu*	---
E4	Sim, o escalão superior da Força Aérea encontra-se envolvido, consciente e procura manter-se sempre atualizado.	11.1
	A informação é transmitida através de relatórios específicos e por meios existentes disponíveis na Força Aérea.	11.2
Q12 - A sua organização cumpre com os requisitos mínimos em termos de ciberdefesa definidos pela NATO [AC/322-D(2017)0047]? Se não, quais os referenciais seguidos pela sua organização na implementação de controlos ou mecanismos de segurança no âmbito da ciberdefesa?		
E1	No âmbito das redes não classificadas não é seguido nenhum referencial em específico, embora se apliquem muitas das boas práticas aí instituídas	12.2
E4	A Força Aérea cumpre com o estipulado pelo CCD para estas matérias, que por sua vez se encontra alinhado com o CCDCOE, Centro de Excelência da NATO, mas nunca esquecendo o preconizado a nível nacional.	12.2 / 12.1
Q13 - Como avalia a necessidade de implementar um processo gestão do risco específico para a realização de ações no ciberespaço?		
E1	Considero ser de elevada importância a implementação de um processo de gestão do risco (…) para desenhar e implementar todos os planos e processos de mitigação e recuperação em caso de ciberincidente	13.1 / 13.2
	conhecida da generalidade da comunidade (…) garantindo um conhecimento permanente das suas capacidades e objetivos inerentes às suas ações no ciberespaço	13.4/ 13.3

E4	Considero ser de elevada importância a implementação de um processo de gestão do risco numa perspetiva de continuidade de serviços e análise de risco à organização.	13.1/ 13.4
	é importante para que as pessoas e a tecnologia estejam devidamente integradas.	13.4
	foi definida uma Política de Continuidade de Serviços de Sistemas de Informação e Tecnologias da Informação e Comunicações da Força Aérea e, que neste momento, está a ser desenvolvido um Plano para o efeito, alinhado com a área de ciber pois os sistemas que são essenciais para o normal funcionamento da organização, bem como para mitigar vulnerabilidades recorrendo aos recursos humanos ou à tecnologia.	13.4/ 13.2
E6	É fundamental	13.1
	Sem dúvida, aliás, os militares sabem fazer isso muito bem. Não se executa operação nenhuma, sem haver primeiro uma avaliação de risco, que condiciona o planeamento da operação e que posteriormente é ajustada e ciclicamente reavaliada antes e ao longo da execução da mesma respetivamente.	13.1
	quando introduzida uma nova tecnologia ou alteração aos recursos humanos, alteramos o panorama do risco	13.4
	A avaliação do risco deve ser uma atividade em permanência, que é suscitada com alteração de pessoas ou de tecnologia	13.4
	G4 é uma estrutura que liga a Defesa, a Cibersegurança, os Serviços de Informações e a Polícia Judiciária (Unidade de Combate ao Cibercrime Tecnológico). Esta estrutura funciona também de forma ad-dock, não tem procedimentos devidamente definidos. Apesar de já ter sido proposta a sua reestruturação, sobretudo quando o nível de ameaça sobe de um patamar para outro, tal ainda não foi concretizada.	3.2
E7	A definição do nível de risco, deverá ter em conta a probabilidade de ocorrência e a severidade/impacto de um ciberataque	5.1
	A articulação da resposta operacional e a própria condução de operações no ciberespaço deverá ter em conta tanto a análise como a gestão do risco associado a cada ciberataque, distinguindo os que, pelo seu nível de severidade, possuem um impacto estratégico e os que, por possuírem um menor poder disruptivo ou destrutivo, não apresentam um impacto tão forte	13.3/ 13.4
	A gestão do risco deve ser contínua.	13.4
Q14 - A condução de operações no ciberespaço deverá ser precedida de uma avaliação do risco? A avaliação do risco deve, sempre que possível, ter em conta uma aferição sistémica do risco?		
E1	Sem dúvida, qualquer ação militar em que domínio seja deve ser precedida de uma análise de risco em função do "terreno" que se pretende explorar	14.1
E4	Sim, a condução de operações no ciberespaço deverá ser precedida de uma avaliação do risco, pois depende de uma estrutura bem montada para dar uma resposta adequada, sendo necessário para tal, ter os recursos essenciais a fim de não parar as dinâmicas da organização.	14.1
	A avaliação do risco deve, sempre que possível, ter em conta uma aferição sistémica do risco dentro das suas competências e capacidades e face ao registo histórico da ciber.	14.2
Q15 - Como profissional na área da ciberdefesa, o que considera prioritário: antecipar as ameaças ou mitigar vulnerabilidades?		
E2	O caminho será, sem dúvida, prevenir os ataques	15.1
	É quase impossível corrigir todas as vulnerabilidades de todos os sistemas e plataformas tecnológicas.	15.1
	O processo de prevenção terá que ser baseado em threat intelligence analysis através de comportamentos de modo a antecipar novos métodos de ataque	15.1
	Deverá existir a capacidade de coletar dados de todos os ativos da organização, e providenciar antecipação das ameaças tendo em conta a análise dos dados.	15.1
	É necessário que com recurso à inteligência artificial faça com que a plataforma consiga lançar investigações forenses num modo automático, analise o incidente e caso seja considerado um verdadeiro positivo, tome ações	15.1
E3	considero que é mais importante antecipar as ameaças (…) só assim poderemos minimizar futuras vulnerabilidades e potenciais ameaças que poderão elevar o risco de segurança.	15.1
	Ao antecipar as ameaças estamos a minimizar o número de vulnerabilidades (…) e desta forma a aumentar o nível de segurança diminuindo o risco.	15.1
E5	Aqui não há prioridades, são tarefas a desempenhar por entidades diferentes e neste caso ambas são prioritárias. Antecipar ameaças faz parte da componente de Cyber Threat Intel (CCD) e mitigar vulnerabilidades das direções técnicas CSI e a Ciberdefesa apoia com uma capacidade de identificação de vulnerabilidades e propostas de mitigação.	15.3/ 15.1/ 15.2

Apêndice E — Matriz de Análise de Conteúdo das Entrevistas Estruturadas - Categorização

UE - Unidades de Enumeração; R - Resultados

Categorias	Subcategorias		Unidades de Registo	Entrevistados							U.E.	R (%)
				1	2	3	4	5	6	7		
Q1 - Com a entrada em vigor das novas LDN e LOBOFA, ambas de 2021, qual o nível de implementação da capacidade de ciberdefesa? Que entidades nacionais colaboram/participam no processo de integração da capacidade de ciberdefesa? Como estão divididas as diferentes responsabilidades de cada entidade? A quem compete tratar o risco?												
Capacidade	Nível de implementação da capacidade de ciberdefesa	1.1	Algumas alterações orgânicas e de nomenclatura face ao anterior	x			x				2	100%
Entidades	Apoio e colaboração	1.2	Ramos				x				1	50%
	Exploração ofensiva	1.3	COCiber	x							1	50%
Tratamento do risco	Competência interna (Ramo)	1.4	Ramos nas operações de cibersegurança.	x							1	50%
	Competência externa (EMGFA)	1.5	EMGFA/ COCiber	x			x				2	100%
Q2 - A edificação da capacidade de ciberdefesa no seio das FFAA, ainda está em processo de consolidação. Comparando o nosso percurso com outros Países e organizações de que Portugal faz parte (NATO e UE), considera que a capacidade de ciberdefesa nacional já possui uma perceção do risco existente no ciberespaço? A atual noção de risco integra a cibersegurança e a ciberdefesa? Como são discriminados os riscos de ciberdefesa, comparativamente aos de cibersegurança?												
Risco	Perceção	2.1	Boa perceção mas com algumas lacunas/constrangimentos, nomeadamente escassez de recursos humanos . Caminho necessário a percorrer.	x			x		x	x	4	100%
	Integração ciberdefesa e cibersegurança	2.2	Cibersegurança e Ciberdefesa integradas				x				1	25%
	Identificação de riscos de ciberdefesa e cibersegurança	2.3	COCiber não desenvolve operações ofensivas no ciberespaço	x							1	25%
Q3 - Conforme noticiado nos órgãos de comunicação social, Portugal tem sido alvo de ciberataques nas mais diversas áreas da sociedade, incluindo na estrutura das FFAA (MDN, EMGFA, etc.). Perante estes acontecimentos, quais os processos e procedimentos usados pela estrutura de ciberdefesa para tratar os riscos?												
Tratamento do risco	Processos (instrumento)	3.1	Autenticação multifator. Framework. Ferramentas CCD.		x			x			2	40%
	Procedimentos (modo)	3.2	Limitar superfície de ataque e aplicar TTP. Normas internas do ramo, CCD e G4.			x		x		x	3	60%
Q4 - Em junho de 2017, a Ucrânia foi alvo de um ciberataque (Malware NotPetya) que infetou computadores de bancos, ministérios, empresas ucranianas, espalhando-se por outras organizações internacionais com escritórios no país, incluindo instituições globais nos setores de transporte marítimo. Qual o papel da ciberdefesa num evento desta envergadura?												
Papel da ciberdefesa perante ataques	Prevenção/ antecipação	4.1	Prevenção.	x					x		2	50%
	Observação/deteção	4.2	Deteção.	x					x		2	50%
	Resposta incidentes	4.3	Resposta	x					x	x	3	75%
	Ação militar	4.4	COCiber						x	x	2	50%

	Outro	4.5	Definido politicamente. Em função do evento. Colaborativo. Intel. Salvaguarda do interesse nacional.	x			x		x	x	4	100%
Q5 - No âmbito da ciberdefesa, como são atualmente identificados os atores e valorizadas as ameaças? A quem compete tal responsabilidade?												
Identificação	Ameaças e Atores	5.1	Difícil, mas tipificados através de várias fontes de Intel e análise forense		x	x		x			3	100%
Valorização	Ameaças	5.2	Feita pelo CCD		x						1	33%
Responsabilidade	Identificar atores	5.3	Não há atribuição de ataques a atores, apenas correlações			x		x			2	67%
	Valorizar ameaças	5.4	CCD					x			1	33%
Q6 - As principais ameaças que se encontram a ser monitorizadas pela ciberdefesa incluem a proliferação de DDOS, ataques à rede elétrica nacional e desinformação? Que outras mais?												
Monitorização e controlo	DDoS	6.1	Acontece com frequência.		x						1	33%
	Rede elétrica nacional	6.2	Responsabilidade do CNCS			x		x			2	67%
	Desinformação	6.3	Responsabilidade do CNCS			x		x			2	67%
	Outros	6.4	Reforço medidas com mecanismos diversos. Ciberdefesa deverá conduzir operações no ciberespaço.		x	x		x			3	100%
Q7 - Considera que a sua organização tem conhecimento suficiente sobre os seus ativos e sobre as suas infraestruturas mais importantes? O atual nível de conhecimento permite aferir vulnerabilidades, implementar controlos de segurança e desenvolver operações no ciberespaço? Que tipo de operações no ciberespaço é a sua organização capaz de desenvolver?												
Nível de conhecimento	Ativos e infraestruturas importantes	7.1	Bom conhecimento de ativos e infraestruturas	x	x	x	x	x			5	100%
	Aferir vulnerabilidades	7.2	Feito com frequência recorrendo a fontes e ferramentas	x	x	x	x				4	80%
	Implementar controlos	7.3	Autenticação multifator.		x						1	20%
	Corrigir vulnerabilidades	7.4	Corrige-se quando necessário	x							1	20%
	Outros	7.5	Ações de suporte (prevenção, deteção, recuperação)		x	x	x				3	60%
Q8 - Na sua organização existe uma monitorização constante das ameaças a que estamos expostos, ou apenas é realizado um registo isolado de eventos/ incidentes de nível Elevado e Crítico? Julga existirem ameaças ou vulnerabilidades, no âmbito de ciberdefesa que não estão a ser tratadas pela sua organização, mas que deveriam? Quais?												
Monitorização e controlo	Constante/ contínua	8.1	Monitorização constante e contínua		x	x		x			3	100%
	Global	8.2	Prioritário de acordo com ameaça. Resultado partilhado.		x	x		x			3	100%
	Isolado	8.3	Prioritário de acordo com ameaça.		x	x		x			3	100%
Falta de controlo e monitorização	Fator humano	8.4	RH são vulnerabilidade (quantidade e qualificações)		x	x		x			3	100%
Q9 - Qual o contributo da sua organização para a determinação do nível de risco percecionado pela ciberdefesa?												
Determinação do nível de risco	Contributos	9.1	Partilha de informação em plataforma de gestão comum. Constante.	x			x		x	x	4	100%
Q10 - Quando ocorre um incidente na sua organização, é produzido algum relatório no âmbito da ciberdefesa? Em caso afirmativo, esse relatório inclui uma avaliação da ameaça ou vulnerabilidade e correspondente estratégia de tratamento do risco? Como flui esta informação dentro da sua organização? Como é feita a comunicação com as demais entidades?												

Ocorrência de incidentes	Reporte/ relatório	10.1	Sim, é feito o registo em plataforma própria.	x	x	x	x	x			5	100%
Relatório reporte incidente	Avaliação da ameaça	10.2	Análise forense		x	x	x	x			4	80%
	Avaliação da vulnerabilidade	10.3	Evidências identificadas.		x	x	x	x			4	80%
	Estratégia de tratamento do risco	10.4	Plano de resposta, mitigação	x	x			x			3	60%
Comunicação	Interna	10.5	Através de plataformas do Ramo/entidade	x				x			2	40%
	Externa	10.6	CCD através de plataforma conjunta	x	x	x	x	x			5	100%
Q11 - Considera existir envolvimento do escalão superior da sua organização na avaliação dos riscos de ciberdefesa? Se sim, de que forma e como é informado o escalão superior?												
Informação superior	Envolvimento chefia militar	11.1	Chefia envolvida, consciente e atualizada				x				1	50%
	Comunicação superior	11.2	Através de relatórios específicos				x				1	50%
Q12 - A sua organização cumpre com os requisitos mínimos em termos de ciberdefesa definidos pela NATO [AC/322-D(2017)0047]? Se não, quais os referenciais seguidos pela sua organização na implementação de controlos ou mecanismos de segurança no âmbito da ciberdefesa?												
Doutrina de controlos de segurança	NATO (AC/322-D(2017)0047)	12.1	Sim, alinhado com práticas do CCD, NATO e Nacional				x				1	50%
	Outros referenciais	12.2	Aplicam boas práticas NATO.	x			x				2	100%
Q13 - Como avalia a necessidade de implementar um processo gestão do risco específico para a realização de ações no ciberespaço?												
Processo de gestão do risco	Necessidade de implementação	13.1	Elevada importância. Fundamental.	x			x		x		3	75%
	Implementar ações mitigação	13.2	Resposta e ações mitigação.	x			x			x	3	75%
	Realização de ações no ciberespaço	13.3	Essencial para realizar ações no ciberespaço	x						x	2	50%
	Outros	13.4	Contínuo e permanente	x					x	x	3	75%
Q14 - A condução de operações no ciberespaço deverá ser precedida de uma avaliação do risco? A avaliação do risco deve, sempre que possível, ter em conta uma aferição sistémica do risco?												
Avaliação do risco	Necessidade de anteceder operações no ciberespaço	14.1	Antes de qualquer ação.	x			x				2	100%
	Aferição sistémica	14.2	Sempre que possível.				x				1	50%
Q15 - Como profissional na área da ciberdefesa, o que considera prioritário: antecipar as ameaças ou mitigar vulnerabilidades?												
Prioridades	Antecipação	15.1	Prevenir e antecipar baseado em Intel para diminuir vulnerabilidades		x	x		x			3	100%
	Mitigação	15.2	Propostas de mitigação					x			1	33%
	Outras	15.3	Não há prioridades, tudo prioritário.					x			1	33%