INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2022/2023

TII

ESCALADA DE CIBERINCIDENTES NAS FORÇAS ARMADAS: ENTIDADES E FUNÇÕES

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.

Miguel Coldron de Tovar Faro

MAJOR, de INFANTARIA "COMANDO"

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ESCALADA DE CIBERINCIDENTES NAS FORÇAS ARMADAS: ENTIDADES E FUNÇÕES

MAJOR, de INFANTARIA "COMANDO" Miguel Coldron de Tovar Faro

Trabalho de Investigação Individual do CEMC 2022/2023

Pedrouços 2023

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ESCALADA DE CIBERINCIDENTES NAS FORÇAS ARMADAS: ENTIDADES E FUNÇÕES

MAJOR, de INFANTARIA "COMANDO" Miguel Coldron de Tovar Faro

Trabalho de Investigação Individual do CEMC 2022/2023

Orientador: CAPITÃO-DE-MAR-E-GUERRA, ENGENHEIRO NAVAL
Sérgio Manuel Ferreira Rodrigues
Coorientador: TENENTE-CORONEL, de ADMINISTRAÇÃO MILITAR
Pedro Manuel Carriço Pinheiro

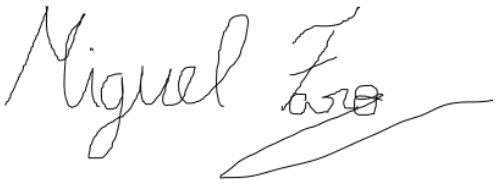
Pedrouços 2023

Declaração de compromisso Antiplágio

Eu, **Miguel Coldron de Tovar Faro**, declaro por minha honra que o documento intitulado "**Escalada de Ciberincidentes nas Forças Armadas: Entidades e Funções"**, corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **CEMC 2022/2023**, 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, **03** de **Maio** de **2023**

Miguel Coldron de Tovar Faro



Agradecimentos

O meu sincero agradecimento aos vários intervenientes que colaboraram, direta e indiretamente, para a realização deste trabalho. Particularmente, ao Tenente-Coronel Jorge Vinagreiro e Capitão-de-Fragata Caldeira Carvalho pelo apoio dado, ao longo do meu estudo, na realização das entrevistas exploratórias, disponibilização de documentação e esclarecimento de dúvidas. Ao Major Silva Monteiro, pela ajuda dada na revisão metodológica do projeto de investigação e pelos esclarecimentos relativos à metodologia durante a elaboração do trabalho. Ao meu orientador, Capitão-de-Mar-e-Guerra Ferreira Rodrigues, e coorientador, Tenente-Coronel Carriço Pinheiro, pela sua constante disponibilidade e apoio ao longo das várias fases de desenvolvimento deste estudo.

Aos camaradas do curso, agradeço profundamente a camaradagem, ajuda e os momentos proporcionados ao longo do curso, que muito contribuíram para o incentivo, essencial, na realização deste trabalho.

Por último, mas não menos importante, um agradecimento especial à minha família pela sua compreensão e sacrifício, ao criarem as condições que me permitiram dedicar o tempo necessário para a realização dos vários trabalhos exigidos pelo curso.

Muito obrigado.

Índice

1. Introdução 1
2. Enquadramento teórico e conceptual 4
2.1 Estado da arte/revisão da literatura 4
2.2 Base conceptual 6
2.1.1 Incidente de segurança das redes e da informação 6
2.1.2 Equipa de resposta a incidentes de segurança informática 6
2.1.3 Escalar da resposta a incidentes 7
2.1.4 *Framework* 7
2.1.5 *National Institute of Standards and Technology* (NIST) 7
2.3 Modelo de análise 8
3. Metodologia e método 9
3.1 Metodologia 9
3.2 Método 10
3.2.1 Participantes e procedimento 10
3.2.2 Instrumento(s) de recolha de dados 10
3.2.3 Técnica(s) de tratamento de dados 11
4. Estrutura, processos e responsabilidades previstas no NIST, na escalada de resposta a ciberincidentes 12
4.1 Síntese conclusiva 19
5. Adequabilidade da estrutura, processos e responsabilidades previstos na lei orgânica do EMGFA (2022), na escalada de resposta a ciberincidentes 21
5.1 Capacidade de resposta a ciberincidentes no EMGFA/COCiber 22
5.2 Capacidade de resposta a ciberincidentes no Exército 31
5.3 Capacidade de resposta a ciberincidentes na Marinha 34
5.4 Capacidade de resposta a ciberincidentes na Força Aérea 36
5.5 Síntese Conclusiva 38
6. Estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes 44
6.1 Cenarização 49

7. Conclusões 52
Referências bibliográficas 55

Índice de Apêndices

Apêndice A – Glossário de conceitos complementares ..... Apd A-1
Apêndice B – Fases do processo de resposta a ciberincidentes ..... Apd B-1
Apêndice C – Modelo de análise ..... Apd C-1
Apêndice D – Metodologia ..... Apd D-1
Apêndice E – Estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes ..... Apd E-1
Apêndice F –Enquadramento da lei orgânica (2022) do EMGFA ..... Apd F-1
Apêndice G –Principais atribuições de algumas entidades das FFAA ..... Apd G-1
Apêndice H – Estrutura, processos e responsabilidades nas FFAA, na escalada de resposta a ciberincidentes ..... Apd H-1
Apêndice I – Lacunas identificadas nas CSIRC do EMGFA e Ramos ..... Apd I-1

Índice de Figuras

Figura 1 - Ciclo de vida da resposta a incidentes 8
Figura 2 - Metodologia científica utilizada na investigação 10
Figura 3 - Comunicação com entidades externas 14
Figura 4 - Estrutura, processos e responsabilidades existentes no NIST, na resposta a ciberincidentes 20
Figura 5 - Macroestrutura do CCICE 22
Figura 6 - Macroestrutura do COCiber 23
Figura 7 - Microestrutura do COCiber, dependências funcionais e técnicas 23
Figura 8 - Macroestrutura do EMCOCiber 25
Figura 9 - Macroestrutura do OPSCiber 26
Figura 10 - Macroestrutura das FOCiber 28
Figura 11 - Macroestrutura do PRTCERTDEF 29
Figura 12 - Macroestrutura do DSCiber 30
Figura 13 - Capacidade de ciberdefesa na estrutura da DCSI do Exército 31
Figura 14 - Capacidade de ciberdefesa do CTms do Exército 33

Figura 15 - Macroestrutura do NuclCIRCEx 34
Figura 16 - Macroestrutura da DITIC, da Marinha 35
Figura 17 - Macroestrutura do NCIRC da Marinha 36
Figura 18 - A capacidade de ciberdefesa na FA 37
Figura 19 - Macroestrutura da DCSI da FA 38
Figura 20 - Macroestrutura da CSIRC do EMGFA 39
Figura 21 - Macroestrutura da CSIRT do Exército 40
Figura 22 - Macroestrutura da CSIRC da Marinha 41
Figura 23 - Macroestrutura da CSIRT da FA 42
Figura 24 - Macroestrutura do GCAD das FFAA, selecionado 44
Figura 25 - Proveniência e ativação das entidades que integrariam o GCAD 45
Figura 26 - Proveniência e ativação das entidades que integram o GCAD 45
Figura 27 - Estrutura CSIRC das FFAA 46
Figura 28 - Acréscimos de responsabilidades (LT, LI e Análise Risco) ao PRTCERDEF, sugeridas 47
Figura 29 - Acréscimos de responsabilidades (EMD) ao PRTCERTDEF, sugerida 47
Figura 30 - Estrutura dos NCIRT dos Ramos, sugerida 48
Figura 31 – Considerações para o plano de reação (ativação) 50
Figura 32 - Considerações para o plano de reação (cenário 1) 50
Figura 33 - Considerações para o plano de reação (cenário 2) 51
Figura 34 - Considerações para o plano de reação (cenário 3) 51
Figura 35 - Esquema sistematizado da metodologia (*Road Map do Tema*) ..... Apd D-1
Figura 36 - Macroestrutura das FFAA ..... Apd F-1
Figura 37 - Macroestrutura do EMGFA ..... Apd F-2

Índice de Quadros

Quadro 1 – Resumo das lacunas identificadas nas FFAA 42
Quadro 2 - Modelo de análise ..... Apd C-1
Quadro 3 - Estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes ..... Apd E-1
Quadro 4 - Estrutura, processos e responsabilidades nas FFAA, na escalada de resposta a ciberincidentes ..... Apd H-1
Quadro 5 - Lacunas identificadas nas CSIRC do EMGFA e Ramos ..... Apd I-1

Resumo

O objetivo deste estudo consiste, em selecionar a estrutura, processos e responsabilidades a serem criados nas Forças Armadas (FFAA) portuguesas, na escalada de resposta a ciberincidentes.

O procedimento utilizado consistiu, exclusivamente, na análise documental clássica para compreensão, comparação e interpretação do *framework* do *National Institute of Standards and Technology* (NIST) e a nova Lei Orgânica das FFAA, identificando possíveis lacunas na organização atual das FFAA, numa escalada de resposta a ciberincidentes.

A nova Lei veio conferir ao Estado Maior General das FFAA (EMGFA) uma maior autoridade técnica e funcional sobre os Ramos, na capacidade de ciberdefesa.

À capacidade *Computer Incident Response Team* (CIRT) do EMGFA devem ser acrescentadas algumas responsabilidades e a criação duma Equipa Modular Destacável. As CIRT dos Ramos, devem passar a ter uma estrutura central e uma maior capacidade e autonomia no tratamento de incidentes, através duma estrutura, articulação e responsabilidades mais idênticas entre si e similares ao CIRT do EMGFA; e o mais próximo do poder de decisão.

Ao nível do EMGFA, deve ser criado um Grupo de Coordenação e Apoio à Decisão, gerindo as entidades envolvidas, para assegurar uma resposta estratégica eficaz das FFAA; e um Plano de Reação, Mitigação e Recuperação de Incidentes.

Palavras-chave: Ciberincidentes; Escalar da Resposta; Forças Armadas Portuguesas; Equipas de Resposta; Responsabilidades.

Abstract

The objective of this study is to select the structure, process and responsibilities to be created in the Portuguese Armed Forces (FFAA), in the escalation of response to cyber incidents.

The procedure used consisted exclusively of classic document analysis for the understanding, comparison and interpretation of the National Institute of Standards and Technology (NIST) framework and the new Organic Law of the FFAA, identifying possible gaps in the current organization of the FFAA, in an escalation of response to cyber incidents.

The new Law of the General Staff of the Armed Forces (EMGFA) has given greater technical and functional authority over the branches in the cyber defense capability.

The EMGFA's Computer Incident Response Team (CIRT) capability should be complemented with some responsibilities and the creation of a Deployable Modular Team. The CIRTs of the branches should have a central structure and greater capacity and autonomy in incident handling, through a structure, articulation and responsibilities that are more identical to each other and similar to the EMGFA's CIRT.

At the EMGFA level, a Coordination and Decision Support Group must be created, managing all the entities involved, to ensure an effective strategic response from the Armed Forces; and an Incident Reaction, Mitigation and Recovery Plan.

Keywords: *Cyber Incidents; Escalation of Response; Portuguese Armed Forces; Response Teams; Responsibilities.*

Lista de abreviaturas, siglas e acrónimos

A

ABWC	Adjunto do *Battle Watch Captain*

B

BTms	Batalhão de Transmissões
BWC	*Battle Watch Captain*

C

CCICE	Centro de Comunicações e Informação, Ciberespaço e Espaço
CCOM	Comando Conjunto para as Operações Militares
CDD	Centro de Dados da Defesa
CEMGFA	Chefe do Estado-Maior General das Forças Armadas
CERT	*Computer Emergency Response Team*
CERT.PT	*Computer Emergency Response Team* Portugal
CFR	Capitão-de-Fragata
CIO	*Chief Information Officer*
CIRC	*Computer Incident Response Center* ou *Computer Incident Response Capability*
CIRT	*Computer Incident Response Team*
CISMIL	Centro de Informações e Segurança Militares
CLAFA	Comando da Logística da Força Aérea
CNCS	Centro Nacional de Cibersegurança
COCiber	Comando de Operações de Ciberdefesa
CSI	Comunicações e Sistemas de Informação
CSIRC	*Computer Security Incident Response Capability*
CSIRT	*Computer Security Incident Response Team*
CTms	Centro de Transmissões

D

DAC	Divisão de Administração de Sistemas e de Comunicações
DCI	Direção de Comunicações e Informação
DCSI	Direção de Comunicações e Sistemas de Informação
DITIC	Direção de Tecnologias de Informação e Comunicações
DIVCSI	Divisão de Comunicações e Sistemas de Informação
DN	Defesa Nacional

DSCiber	Departamento de Sistemas de Ciberdefesa
DSE	Divisão de Suporte aos Serviços e Sistemas em Exploração
E	
EFMCiber	Equipas das Forças de Missão do Ciberespaço
EM	Estado-Maior
EMCOCiber	Estado-Maior do COCiber
EMD	Equipa Modelar Destacável
EMGFA	Estado Maior General das Forças Armadas
ETIR	Equipa Técnica de Intervenção Rápida
F	
FA	Força Aérea
FFAA	Forças Armadas
FOCiber	Forças de Operações de Ciberdefesa
G	
GCAD	Grupo de Coordenação e Apoio à Decisão
GPNS	Gabinete de Projetos, Normalização e Segurança
GRISI	Grupos de Reação a Incidentes de Segurança Informática
I	
I&D	Investigação e desenvolvimento
IP	*Internet Protocol*
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
ISP	*Internet Service Providers*
ISR	Informações, Vigilância e Reconhecimento (*Intelligence, Surveillance and Reconnaissance*)
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission* (Organização Internacional de Normalização/Comissão Eletrotécnica Internacional)
IWC	*Intel Watchkeeper*
L	
LA	Lições Aprendidas
LEGAD	*Legal Adviser*
LI	Líder de Incidente

LOEMGFA	Lei Orgânica do Estado-Maior-General das Forças Armadas
LT	Líder Técnico
M	
MDN	Ministério da Defesa Nacional
MMHS	*Military Message Handling System*
ModTatCIRC	Módulo Tático CIRC
N	
NATO	*North Atlantic Treaty Organization*
NCIRC	Núcleo *Computer Incident Response Capability*
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
O	
OE	Objetivo Específico
OG	Objetivo Geral
OPSCiber	Centro de Operações no Ciberespaço
OTAN	Organização do Tratado do Atlântico Norte
P	
p. ex.	Por Exemplo
PJ	Polícia Judiciária
POC	Ponto de Contato
PRTCERTDEF	Centro de resposta a incidentes da Defesa
Q	
QC	Questão Central
QD	Questão Derivada
R	
RSI	Repartição de Sistemas de Informação
RTI	Repartição de Tecnologias de Informação
S	
SegInf	Segurança da Informação
SI	Sistemas de Informação
SIS	Serviço de Informações de Segurança
SOP	*Standard Operating Procedures*
SSTI	Secção de Suporte a Sistemas de Tecnologias de Informação

T

TCOR	Tenente-Coronel
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicações

V

Vs	*Versus*

1. Introdução

O Ciberespaço assume-se como um domínio transversal a todos os outros domínios (North Atlantic Treaty Organization [NATO], 2022), contudo, suscetível de ser explorado por novas formas de ameaça, estatais e não estatais, de impacto transversal e de natureza transnacional, pela execução de ataques e crimes no mundo virtual. Não apenas a privacidade e liberdade dos cidadãos pode ser invadida através da prática de Cibercrimes, como também, a própria soberania do Estado, uma vez que, a informação capturada pode ameaçar a segurança nacional ou a sobrevivência das principais instituições de poder do Estado. A crescente relevância do Ciberespaço para o exercício da soberania e defesa dos interesses nacionais, demonstra uma necessária visão política, clara e coerente, que permita a definição de objetivos para a edificação conducente das capacidades nacionais neste domínio. A edificação de capacidades nacionais em ciberdefesa e cibersegurança, torna-se essencial nas Forças Armadas (FFAA) para uma adequada resposta multidimensional, civil-militar e nacional-internacional, perante as vulnerabilidades existentes (Santos, Nunes, Ralo, & Mendes, 2018).

Existem inúmeros casos públicos de ciberataques dirigidos a diferentes organizações e Estados, bem como, é publico e reconhecido a insuficiente preparação de muitas organizações, internacionais e nacionais, para lidar com ciberataques. Os ataques são cada vez mais frequentes, diversificados e os seus efeitos mais disruptivos, com impacto nos vários setores da sociedade e na vida das populações. Os riscos aumentam em função da maior digitalização das sociedades e da dependência da tecnologia e infraestruturas tecnológicas, expostas a ataques e ameaças cada vez mais especializadas e evoluídas. As falhas de segurança estão presentes nas organizações, estas, simplesmente ainda não as descobriram ou revelaram terem sido alvo de ataques (Matos, 2018, pp. 1-2).

Esta realidade também se verifica em várias organizações nacionais, inclusive nas FFAA, exigindo a estas a preparação e capacitação para uma adequada gestão de incidentes, através de um processo que permita uma resposta pronta, clara e eficiente, para assegurar a proteção dos seus ativos (pessoas, dados e processos) de uma forma reativa, mas também preventiva (Matos, 2018, pp. 1-2 e 55).

Nem todos os incidentes podem ser prevenidos, pois estão frequentemente a surgir novos tipos de incidentes relacionados com a segurança. Contudo, é possível reduzir o número de incidentes através de atividades preventivas, com base nos resultados das avaliações de risco. Para tal, é necessária uma capacidade de resposta a incidentes para

permitir, de uma forma rápida, detetar incidentes, identificar a origem e objetivos, conter/minimizar perdas e destruição, mitigar as fraquezas que foram exploradas e restaurar os serviços afetados (National Institute of Standards and Technology [NIST], 2012, p. 1).

A resposta a incidentes de segurança informática tornou-se uma componente importante dos programas de tecnologia da informação (TI). O seu desempenho eficaz é uma tarefa complexa, tal como o processo de edificação de uma capacidade de resposta, pois requerem um planeamento e recursos substanciais (NIST, 2012, p. 1).

O ciberataque realizado às FFAA, em agosto de 2022, faz-nos interrogar se estas estarão preparadas, ao nível da sua estrutura, coordenação e processos, para responder a incidentes que escalem no domínio da ciberdefesa/cibersegurança, enfatizando assim o **problema estudado** nesta investigação.

O Decreto-Lei n.º 19/2022, de 24 de janeiro, veio estabelecer a nova Lei Orgânica do Estado-Maior-General das Forças Armadas (LOEMGFA) e alterar as Leis Orgânicas dos três Ramos das FFAA, dando uma maior responsabilidade e funções de coordenação à estrutura do Estado-Maior-General das Forças Armadas (EMGFA) sobre os Ramos, inclusive ao Comando de Operações de Ciberdefesa (COCiber), recentemente criado, que passa a ter autoridade técnica e funcional, na capacidade de ciberdefesa, sobre os Ramos. Assim, passa a existir uma maior influência e coordenação entre o *Computer Incident Response Team* (CIRT) do EMGFA e o CIRT dos Ramos.

Tendo por base a forma como é executada a escalada de ciberincidentes, prevista na resposta das FFAA portuguesas, em comparação à *Framework* de boas práticas de resposta a incidentes do NIST, pretende-se analisar, se a nova organização das FFAA prevê a estrutura, processos e responsabilidades adequadas na escalada de resposta a ciberincidentes, identificando-se possíveis lacunas na organização atual. Assim, torna-se importante este estudo que irá contribuir para as FFAA, nomeadamente, para o COCiber, através da sugestão de melhorias para a capacidade de resposta a ciberincidentes.

Esta investigação tem como objeto de estudo a estrutura, processos e responsabilidades, do EMGFA e dos Ramos, a serem criados na escalada de resposta a ciberincidentes, face à nova organização das FFAA, prevista em 2022. O estudo está delimitado:

- Espacialmente, a Portugal.
- Conteúdo, à estrutura, processos e responsabilidades do EMGFA e dos Ramos, com base na nova LOEMGFA.

- Temporalmente, de 24 de janeiro de 2022 (data da nova LOEMGFA) a junho de 2023 (mês no qual será executada a exposição oral deste trabalho).

O Objetivo Geral (OG) deste estudo é **selecionar a estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes**.

A partir do OG, foram definidos dois Objetivos Específicos (OE):

- OE1: **Identificar** a estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes.
- OE2: **Analisar** a adequabilidade da estrutura, processos e responsabilidades previstos na nova LOEMGFA, na escalada de resposta a ciberincidentes.

Com base no OG estabelecido, definiu-se a seguinte Questão Central (QC): Que estrutura, processos e responsabilidades devem ser criados nas FFAA, na escalada de resposta a ciberincidentes?

A partir da QC, definiram-se as seguintes Questões Derivadas (QD):

- QD1: Qual a estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes?
- QD2: De que forma a estrutura, processos e responsabilidades previstos na nova LOEMGFA, na escalada de resposta a ciberincidentes se encontram adequados?

Este documento está organizado em sete capítulos. Além da Introdução e Conclusão, no Capítulo 2 efetua-se o enquadramento teórico e conceptual, os principais conceitos estruturantes e o modelo de análise do trabalho. No Capítulo 3, explica-se a metodologia e o método utilizados na investigação. No Capítulo 4, identifica-se o modelo de referência da estrutura, processos e responsabilidades na resposta a ciberincidentes do NIST, dando-se resposta à QD1. No Capítulo 5, com base na nova LOEMGFA, analisa-se a existência de lacunas na organização atual das FFAA, comparativamente ao NIST, na resposta a ciberincidentes, dando-se resposta à QD2. No Capítulo 6, a partir das lacunas identificadas seleciona-se a estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes, dando-se resposta à QC.

2. Enquadramento teórico e conceptual

Este capítulo começa por identificar, em que medida este estudo se distingue de outros já realizados. Posteriormente, definem-se os conceitos estruturantes do trabalho. No final, apresenta-se o modelo de análise.

2.1 Estado da arte/revisão da literatura

Este estudo situa-se no contexto das Ciências Militares, na área das Técnicas e Tecnologias Militares e na subárea da cibersegurança.

Em 2010, Francisco Lopes na sua dissertação, associada ao tema "Gestão do conhecimento – Modelação dos Incidentes e das Respostas", focando a sua análise nos sistemas de aprendizagem de incidentes na segurança da informação, estuda o efeito de determinadas variáveis de gestão no desempenho das organizações, pela medição da taxa de ocorrência de incidentes.

Comprovou que as empresas só partilham o conhecimento se identificarem vantagens nessa ação; que a cultura organizacional é determinante na partilha do conhecimento e na definição de poderes; e que a gestão de incidentes contribui para a deteção, registo e investigação de incidentes, no apoio à mitigação de riscos, permitindo a inexistência de falhas.

Concluiu que há muitas dificuldades a superar para implantar sistemas de aprendizagem funcionais; que as quantidades de notificação de incidentes podem ser enganadores, sendo necessário medir a cultura de segurança e o grau de severidade dos incidentes; é mais produtivo o enfoque na melhoria da cultura de notificação, ao remover recriminações do que ao aumentar incentivos; e que os colaboradores não-técnicos têm de ser mantidos no ciclo.

Neves e Correia (2016) no seu artigo, com o tema "Resposta a Incidentes de Segurança da Informação: Uma abordagem DOTMLPI-I", focam-se na identificação dos elementos críticos a considerar na edificação de uma capacidade de resposta a incidentes de segurança da informação no ciberespaço, aplicando a metodologia da Organização do Tratado do Atlântico Norte (OTAN) para a edificação de capacidades operacionais.

Consideram que a cibersegurança é executada na capacidade de antecipar e responder a ciberincidentes que afetam a informação que circula no ciberespaço nacional.

Concluíram, como elementos críticos ao nível da Doutrina, os princípios legislativos no enquadramento da ação da equipa de resposta a incidentes relativamente aos objetivos e âmbito de atuação; ao nível da Organização, a articulação e comunicação dentro da

capacidade; ao nível do Treino, os exercícios para o desenvolvimento de competências no âmbito da decisão, coordenação, partilha de informação e capacidades técnicas; ao nível do Material, os meios necessários para monitorização, deteção e registo de eventos que poderão escalar em incidentes; ao nível da Liderança; o envolvimento dos níveis superiores de chefia em todo o processo, dotando os recursos humanos e materiais necessários; ao nível do Pessoal, a formação e treino para serem alcançados os objetivos da Doutrina e a estabilidade das equipas; ao nível da Interoperabilidade, a atuação integrada de várias entidades para mitigar os riscos, partilhar informação e conhecimentos, e para o conhecimento situacional do Ciberespaço. Esta última, vital, na qual só pode ser materializada com a existência de mecanismos de comunicação compatíveis, relações sólidas e de confiança entre os vários atores de cibersegurança.

Em 2018, Daniel Matos na sua dissertação, associada ao tema "Gestão de Incidentes de Cibersegurança em Organizações Públicas", aborda a problemática das organizações públicas estarem suficientemente preparadas para gerirem incidentes de cibersegurança, baseando-se nas *frameworks* de normas e guias de boas práticas da *European Union Agency for Cybersecurity*, do NIST e *International Organization for Standardization* (ISO).

O seu estudo, foca-se na proposta de um método que concretiza um processo de referência para a gestão de incidentes de cibersegurança, constituído por cinco fases (Planeamento e Preparação, Deteção e Participação, Análise e Avaliação, Resposta e Documentação, e Lições Aprendidas - LA).

Conclui, que a gestão de incidentes deve ser feita de forma metódica, estruturada e deve envolver a organização como um todo, na qual o seu comprometimento e sustentação deve ser gerido pelo topo da organização; que as organizações publicas e privadas portuguesas, ainda não estão suficientemente preparadas para gerir este tipo de incidentes, perante a cada vez maior sofisticação dos ciberataques, devendo capacitarem-se para tal adotando um processo de gestão; que os comportamentos inadequados dos utilizadores são as principais causas dos incidentes; e se as organizações adotarem um normativo internacional reconhecido, neste caso o *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27035, traz vantagens de harmonização e interoperabilidade.

O atual estudo, apesar de ter em comum a utilização de uma *framework* de referência de boas práticas, irá diferir dos anteriores, por focar a sua análise nas FFAA, no âmbito da

estrutura, processos e responsabilidades na escalada de resposta a ciberincidentes, à luz do novo Decreto-Lei.

2.2 Base conceptual

Neste subcapítulo apresentam-se os conceitos estruturantes do trabalho. Os conceitos complementares, encontram-se no Apêndice A.

2.1.1 Incidente de segurança das redes e da informação

De acordo com Daniel Matos é:

> […] uma ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores que resulta, ou pode resultar, na perda da confidencialidade ou integridade da informação ou prejudica o desempenho de uma rede de comunicação de dados ou sistema. Normalmente um incidente de segurança das redes e da informação significa uma violação da política de segurança de uma organização. (2018, p. 8)

Segundo o NIST (2012, p. 6), é uma violação, ou ameaça iminente de violação, das políticas de segurança informática, políticas de utilização aceitável ou práticas de segurança padrão[1].

2.1.2 Equipa de resposta a incidentes de segurança informática

Segundo a Lei n.º 46/2018, de 13 de agosto é:

> […] A equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma organização, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação. (2018, p. 4031)

De acordo com o NIST (2012, p. 60), é uma capacidade criada com o objetivo de ajudar na resposta a incidentes relacionados com a segurança informática; também denominada CIRT ou CIRC (*Computer Incident Response Center*, *Computer Incident Response Capability*)[2].

[1] Tradução do autor de "*A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*".
[2] Tradução do autor de "*A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).*".

Estas Equipas, também podem ser designadas de *Computer Security Incident Response Team* (CSIRT), *Computer Emergency Response Team* (CERT) ou *Computer Security Incident Response Capability* (CSIRC).

2.1.3 Escalar da resposta a incidentes

Neste trabalho, considera-se escalar da resposta a incidentes, quando o nível subordinado não responde a um incidente local dentro do tempo estimado, por não ter capacidade para tal, pela gravidade do incidente ou pelo risco dos seus efeitos se alastrarem às FFAA, passando a resposta ao incidente a ser executada pelo nível superior.

2.1.4 Framework

É um "Modelo de referência." (Centro Nacional de Cibersegurança [CNCS], 2019b, p. 17).

2.1.5 *National Institute of Standards and Technology* (NIST)

O NIST é a entidade responsável pelo desenvolvimento de normas, requisitos (dos sistemas) e diretrizes de segurança da informação; por promover a economia e o bem-estar público, fornecendo a liderança técnica na criação de medidas e normas para as infraestruturas dos Estados Unidos da América (NIST, 2012, pp. ii, 1 e 4).

A 2ª revisão da sua publicação especial 800-61, intitulada *Computer Security Incidente Handling Guide* (2012), é um guia de boas práticas que indica metodologias para a edificação de uma capacidade de resposta a incidentes de segurança da informação (Neves & Correia, 2016). Tendo como foco principal a deteção, análise, priorização e tratamento de incidentes, fornece orientações práticas sobre análise de dados, mitigação de riscos e como responder a incidentes de forma eficaz e eficiente. Este guia destina-se às CSIRT, sistemas e administradores de rede, pessoal de segurança e de apoio técnico, *Chief Information Security Officer*, *Chief Information Officer* (CIO), gestores de programas de segurança informática e outros responsáveis pela preparação ou resposta a incidentes (NIST, 2012, pp. 1 e 4).

O seu **processo** de resposta a incidentes é composto pelas fases da preparação; deteção e análise; contenção, erradicação e recuperação; e atividade pós-incidente (NIST, 2012, p. 21). A explicação de cada uma destas fases está vertida no Apêndice B.

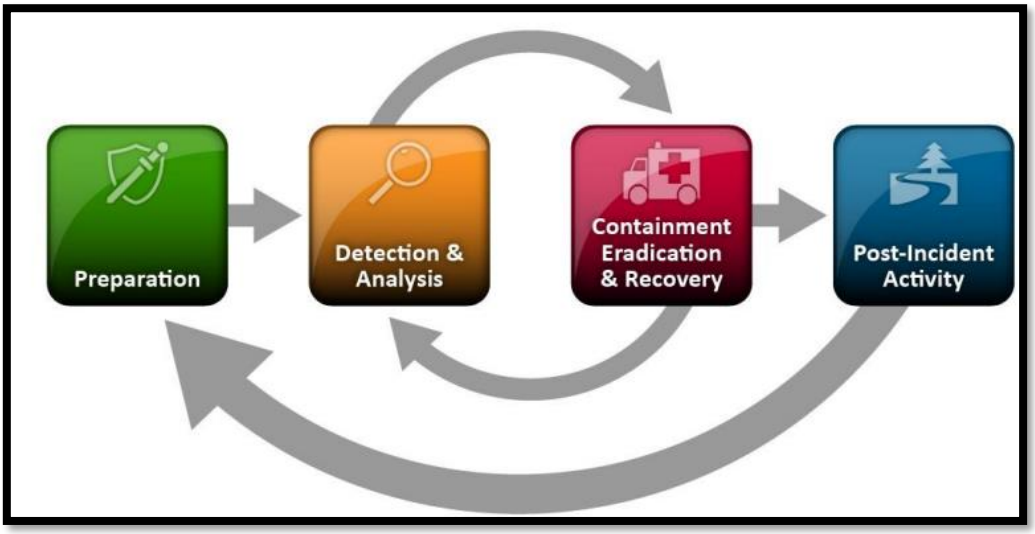


Figura 1 - Ciclo de vida da resposta a incidentes

Fonte: NIST (2012, p. 21).

Uma das recomendações do NIST relaciona-se com as ações a adotar pela organização para criar, fornecer e operar uma capacidade de resposta formal a incidentes. Este estudo centraliza-se, maioritariamente, na ação de seleção de uma estrutura de equipa de resposta e no modelo de pessoal da equipa (além do processo de resposta a incidentes) (NIST, 2012, pp. 1-2).

2.3 Modelo de análise

Para orientação do estudo foi elaborado o modelo de análise constante no Apêndice C, que define como:

- Conceitos Estruturantes: Ciberincidentes, equipa de resposta, escalada da resposta, *framework* NIST.
- Dimensões: A escalada da resposta a ciberincidentes no NIST e nas FFAA.
- Indicadores: Os processos, responsabilidades, órgãos, funções, entidades, grupos de tomada de decisão envolvidos na resolução de incidentes.

3. Metodologia e método

De seguida, explica-se a metodologia e o método utilizado para realização desta investigação.

3.1 Metodologia

A metodologia de investigação adotada tem em consideração as Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (Santos & Lima, 2019) e as normas vigentes do Instituto Universitário Militar (NEP/INV - 001 (A1), 2020); NEP/INV - 003 (A3), 2020).

Tendo como referência a *framework* de boas práticas de resposta a incidentes do NIST, procurou-se identificar a estrutura, processos e responsabilidades existentes nesse modelo de referência, numa escalada de resposta a ciberincidentes. Posteriormente, efetuou-se uma análise da nova LOEMGFA (2022), para verificar a adequabilidade da estrutura, processos e responsabilidades das FFAA portuguesas, na escalada de resposta a ciberincidentes, comparativamente ao NIST, identificando, a partir destas duas dimensões, possíveis lacunas na organização atual do EMGFA e dos Ramos. Com base nas lacunas, selecionou-se dedutivamente (tendo em referência o NIST) o processo, estrutura e responsabilidades a serem criados nas FFAA, na escalada de resposta a Ciberincidentes (Apêndice D).

Como demonstrado, o desenho de pesquisa adotado foi o estudo de caso das FFAA/COCiber, no qual o conhecimento originado resultou da perspetiva interpretativa dessa realidade (Santos & Lima, 2019, p. 37), num horizonte temporal transversal, de 2022 a 2023.

Ao longo de todo o percurso metodológico utilizou-se um raciocínio dedutivo, a partir de uma "lei geral" (*framework* NIST) para o particular (aplicada às lacunas identificadas na organização atual das FFAA); e uma estratégia de investigação qualitativa (Santos & Lima, 2019, pp. 19 e 128).

A recolha e análise de dados foi feita através da análise documental (Santos & Lima, 2019, p. 29).

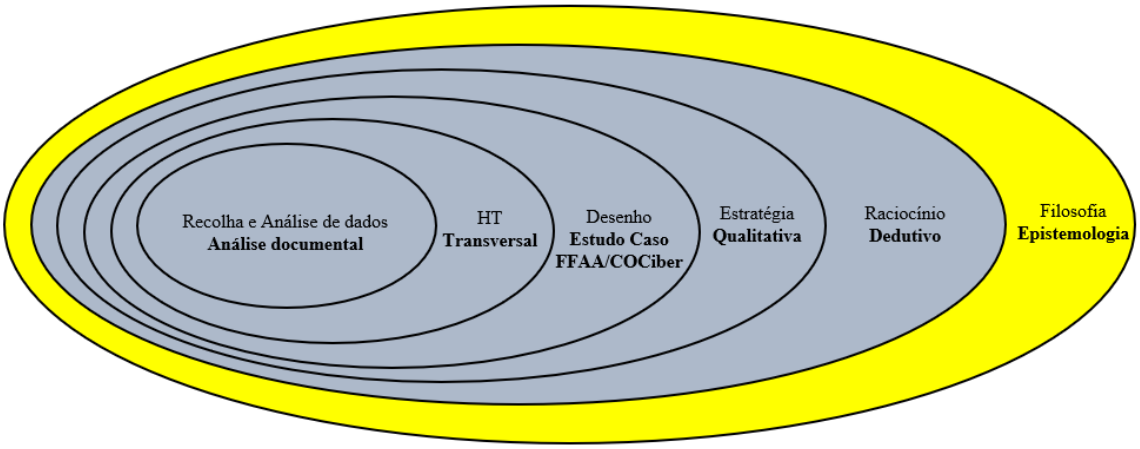


Figura 2 - Metodologia científica utilizada na investigação

Fonte: Adaptado a partir de Santos & Lima (2019).

3.2 Método

3.2.1 Participantes e procedimento

Os participantes na investigação, numa fase exploratória, foram o Chefe de Estado Maior (Capitão-de-Fragata – CFR – Caldeira Carvalho) e o Comandante das Forças de Ciberdefesa (Tenente-Coronel – TCOR - Vinagreiro), do COCiber.

O procedimento utilizado consistiu, numa primeira fase, na realização de entrevistas exploratórias, no COCiber, e na pesquisa bibliográfica para compreender o estado da arte e identificar a problemática. O contato inicial foi feito por email e telefone, para agendamento das respetivas entrevistas. Estas, foram realizadas por telefone, ao CFR Carvalho, e presencialmente, ao TCOR Vinagreiro.

Numa segunda fase, o procedimento consistiu exclusivamente na análise documental com a finalidade de compreender e interpretar as duas dimensões em análise, a *framework* do NIST e a nova LOEMGFA, em resposta às QD e QC.

3.2.2 Instrumento(s) de recolha de dados

A recolha de dados foi feita, inicialmente, através de entrevistas exploratórias semiestruturadas (Pardal & Correia, 1995, cit. por Santos & Lima, 2019, p. 84).

Posteriormente foi utilizada a análise documental (Sousa & Baptista, 2011, cit. por Santos & Lima, 2019, p. 29) em fontes abertas nacionais, maioritariamente, artigos científicos e trabalhos de investigação académicos no âmbito da resposta a ciberincidentes,

para permitir a compreensão dos principais conceitos e a seleção de um *framewok* de boas práticas.

Foram utilizadas fontes abertas não-nacionais, nomeadamente, o *Computer Security Incident Handling Guide* do NIST, para compreensão desta *framework* e identificação dos processos, estrutura e responsabilidades envolvidas numa reposta a ciberincidentes.

Por último, foram utilizados manuais de referência de cibersegurança do CNCS e documentos legislativos como a Resolução do Conselho de Ministros nº106/2022, que aprova a Estratégia Nacional de Ciberdefesa, e o Decreto Lei nº19/2022, que estabelece a Lei Orgânica das FFAA e altera as Leis Orgânicas dos três Ramos das FFAA, com a finalidade de analisar a nova organização atual das FFAA.

3.2.3 Técnica(s) de tratamento de dados

O tratamento dos dados recolhidos da análise documental, foi feita através da técnica documental clássica (Santos & Lima, 2019, p. 93).

4. Estrutura, processos e responsabilidades previstas no NIST, na escalada de resposta a ciberincidentes

Este capítulo procura identificar a estrutura, processos e responsabilidades previstas no modelo de referência do NIST, numa resposta a ciberincidentes.

Para uma resposta a incidentes eficaz, além do planeamento e recursos substanciais, é essencial uma capacidade de monitorização contínua e o estabelecer procedimentos claros, que permitam a priorização do tratamento de incidentes. Requer também, a implementação de métodos eficazes de recolha, análise e comunicação de dados. Por último, é vital construir relações e estabelecer meios de comunicação adequados com outros grupos internos (p. ex. com os recursos humanos ou com o *Legal Adviser* – LEGAD) e com grupos externos (p. ex. outras equipas de resposta a incidentes ou forças de segurança) (NIST, 2012, p. 1).

Um CSIRC permite (NIST, 2012, pp. 6-7):

- Apoiar com uma resposta sistemática a incidentes (seguindo uma metodologia de tratamento de incidentes) para que sejam tomadas as medidas apropriadas;
- Ajudar o pessoal a minimizar a perda ou roubo de informação e a interrupção dos serviços;
- Utilizar a informação obtida, durante o tratamento de incidentes, para melhor preparação do tratamento de futuros incidentes;
- Proporcionar uma proteção mais robusta aos sistemas e dados;
- Lidar de forma mais adequada com as questões legais, que possam surgir durante os incidentes;
- Assegurar o cumprimento das leis, dos regulamentos e políticas que dirigem uma defesa, coordenada e eficaz, contra ameaças à segurança da informação.

Para se organizar um CSIRC, a organização deve decidir sobre quais os serviços a serem prestados pela equipa de resposta, qual a estrutura e modelo das equipas necessário para prestar esses serviços, de modo a serem selecionadas e implementadas uma ou mais equipas. O estabelecimento da equipa requer a criação de planos, políticas e procedimentos de resposta eficazes, eficientes e consistentes, que reflitam as interações da equipa com outras equipas dentro da organização e com entidades externas, mas também, para que a equipa esteja habilitada a fazer o que lhe compete (NIST, 2012, p. 6).

Alguns dos elementos da política de resposta a incidentes, são (NIST, 2012, pp. 7-8):

- A estrutura organizacional e a definição de papéis, responsabilidades e níveis de autoridade. Aqui, devem ser incluídas a autoridade da equipa de resposta

para confiscar ou desligar equipamentos e monitorizar atividades suspeitas, os requisitos para a comunicação de certos tipos de incidentes, os requisitos e orientações para comunicações externas e partilha de informação (o que pode ser partilhado, com quem, quando e quais os canais a utilizar) e os pontos de transição e escalonamento no processo de gestão de incidentes;

- Classificação de gravidade ou priorização dos incidentes;
- Medidas de desempenho.

A missão, estratégias e objetivos da organização, devem auxiliar a determinar o tipo de estrutura da sua capacidade de resposta a incidentes (NIST, 2012, p. 8).

O plano de resposta a incidentes deve promover o *roadmap* para a implementação da capacidade de resposta, de acordo com os requisitos da organização. Os requisitos são de acordo com a missão, dimensão, estrutura e funções da organização. Assim que uma organização desenvolve um plano e obtém a aprovação da gestão, deve implementar o plano e revê-lo, pelo menos anualmente, para assegurar que está a seguir o *roadmap* para a maturação da capacidade e o cumprimento dos seus objetivos de resposta (NIST, 2012, p. 8).

Os procedimentos devem basear-se na política e no plano de resposta a incidentes. Os *Standard Operating Procedures* (SOP) traduzem os processos técnicos específicos, técnicas, listas de verificação e formulários utilizados pela equipa de resposta. Devem ser abrangentes e detalhados, para assegurar que as prioridades da organização são refletidas nas operações de resposta, minimizando os erros através de repostas *standart*. Os SOP devem ser testados, validados e distribuídos a todos os membros da equipa, ministrando a sua formação aos utilizadores (NIST, 2012, pp. 8-9).

A comunicação com entidades externas, relativamente a um incidente, deve ser feita de forma apropriada e pode ocorrer por diferentes motivos: para partilha de informação (com os serviços de segurança, meios de comunicação social…), procura de entidades com conhecimento especializado e discussão de incidentes com outras partes envolvidas. Neste último caso, o reporte de um incidente (o contato deve ser feito por intermédio do CERT Nacional) poderá ser com os *Internet Service Providers* (ISP) (p. ex. eventuais necessidades de assistência), proprietários de endereços de ataque (p. ex. eventuais recolhas de prova, caso os ataques corram a partir de um endereço de um *Internet Protocol* – IP – externo), vendedores de software (p. ex. recolha de informação sobre ameaças e novas formas de ataque), outras equipas de resposta a incidentes (p. ex. para desenvolvimento do

conhecimento situacional) e entidades externas afetadas (p. ex. para notificar organizações externas afetadas pelo ataque) (NIST, 2012, pp. 9, 12-13).

A partilha proativa de informações relevantes, sobre indicadores de incidentes, contribui para melhorar a deteção e análise de incidentes. A equipa de resposta deve discutir a partilha de informação com o gabinete de assuntos públicos da organização, o departamento jurídico e a direção, antes que um incidente ocorra, para estabelecer políticas e procedimentos relativos à partilha de informação, de modo que, a informação sensível não seja fornecida a entidades não autorizadas (*need to know basis*). Todos os contactos e comunicações com partes externas devem ser documentados, para efeitos de responsabilização e fins probatórios (NIST, 2012, p. 9).

Figura 3 - Comunicação com entidades externas

Fonte: NIST (2012, p. 10).

Para discutir incidentes com os meios de comunicação social, a organização pode pretender a participação dos elementos do seu gabinete de assuntos públicos e departamento jurídico. Frequentemente, considera-se benéfica a designação de um ponto de contacto (POC) principal e um alternativo (NIST, 2012, p. 10).

Muitos incidentes relacionados com a segurança não resultam em condenações, devido a algumas organizações não contactarem devidamente as autoridades de segurança. Estas, existem a vários níveis para investigar incidentes e podem ser envolvidas agências de segurança de outros países, caso os ataques sejam dirigidos/executados a partir desses. A equipa de resposta deve estar familiarizada com as várias entidades de segurança, antes da ocorrência de um incidente, para definir as condições em que os incidentes são comunicados, como é feita a comunicação, que provas devem ser recolhidas e como estas devem ser

recolhidas. Preferencialmente, nomeia-se um elemento da equipa como o POC principal para as forças de segurança, devendo este estar preparado para recomendar a força de segurança a contatar (NIST, 2012, p. 11).

A legislação obriga a que as agências reportem os incidentes para o CERT Nacional, enquanto ponto focal para lidar com os incidentes. Este, vai analisar a informação reportada para identificar indicadores e tendências dos ataques. As organizações devem encorajar o reporte de incidentes para os seus respetivos CSIRT. Deve haver um POC principal e secundário para o CERT Nacional, assegurando o reporte de todos os incidentes de acordo com as políticas de resposta definidas (NIST, 2012, pp. 11-12).

Uma equipa de resposta deve estar disponível para qualquer elemento da organização que detete ou desconfie da ocorrência de um incidente. O efetivo desta equipa varia de acordo com a magnitude do incidente e a disponibilidade de pessoal. Cabe a esta equipa analisar os dados do incidente, determinar o seu impacto, agir adequadamente para limitar os danos e restaurar os serviços normais. O seu sucesso está dependente da participação e cooperação dos indivíduos de toda a organização (NIST, 2012, p. 13).

Existem diferentes modelos de estrutura de uma equipa de resposta a incidentes (NIST, 2012, p. 13):

- Equipa de Resposta a Incidentes Central, consiste numa equipa singular para lidar com os incidentes de toda a organização. É mais eficaz em organizações pequenas e com menor diversidade geográfica de recursos informáticos.
- Equipa de Resposta a Incidentes Distribuída, consiste em múltiplas equipas de resposta em toda a organização, em que cada equipa é responsável por um segmento particular (lógico ou físico) da organização. É mais eficaz em organizações grandes (p. ex. uma equipa por divisão) e com maior diversidade geográfica de recursos informáticos (p. ex. uma equipa por região geográfica). Neste modelo, as equipas devem integrar uma única entidade de coordenação, de modo a garantir a consistência do processo de resposta em toda a organização e a partilha da informação entre as várias equipas.
- Equipa de Coordenação, em que uma equipa de resposta fornece aconselhamento a outras equipas, sem ter autoridade sobre elas. Este modelo, deve ser pensado como sendo um CSIRT para outros CSIRT.

As equipas de resposta a incidentes podem utilizar três modelos de composição de pessoal (NIST, 2012, p. 14):

- Funcionários, em que a organização realiza todo o seu trabalho de resposta a incidentes com um limitado apoio (técnico e administrativo) de pessoal externo contratado.
- Parcialmente *Outsourced*, em que a organização subcontrata pessoal para executar parte do trabalho de resposta a incidentes.
- Totalmente *Outsourced*, em que a organização subcontrata todo o seu trabalho de resposta a incidentes. Normalmente, é usado este modelo quando a organização necessita de uma equipa de resposta a tempo integral e não tem funcionários suficientes, disponíveis e qualificados para tal.

Na seleção do modelo de equipa, as organizações devem ter em conta os seguintes fatores (NIST, 2012, pp. 14 e 15):

- A necessidade de disponibilidade 24/7 das equipas de resposta, seja na modalidade de ativação por telefone ou através de presença local permanente.
- Membros da equipa a tempo Integral *versus* tempo parcial, normalmente, para organizações com limitado financiamento, pessoal ou necessidade de resposta, na qual é suficiente a existência de equipas de resposta a tempo parcial, servindo como uma equipa de resposta virtual. Aquando de uma emergência, a equipa é contatada a fim de prestar assistência. Um *help desk* de TI, poderá servir como um POC inicial para reporte de incidentes.
- O moral dos funcionários, tendo em conta que o trabalho de resposta é extremamente stressante, agravado ainda mais com as necessidades de permanência integral. Deste fator, advêm dificuldades em encontrar pessoas dispostas, disponíveis, experientes e qualificadas para integrar estas equipas, particularmente, no apoio 24/7. A segregação de funções, nomeadamente, reduzir a quantidade de trabalho administrativo dos elementos da equipa de resposta, pode ser uma ajuda.
- Os custos são sempre um fator de relevo, principalmente para os elementos da equipa em permanência 24/7. Devem ser incluídos pela organização, os custos associados às necessidades de formação e manutenção das competências destas equipas (considerando que precisam de conhecimentos mais amplos do que o pessoal das TI) e os custos associados à segurança física (áreas de trabalho da equipa e mecanismos de comunicação).

- A especialização do pessoal, uma vez que, o tratamento de incidentes requer conhecimentos especializados e experiência em várias áreas técnicas. O pessoal pertencente à organização geralmente tem um conhecimento maior do ambiente da organização, comparativamente a um *outsourcer*.

As equipas de resposta, num modelo *outsourcing*, são compostas por um funcionário com um ou dois reservas, nomeados para supervisionar e avaliar o trabalho dos elementos *outsourcer*. Para os restantes modelos, normalmente a equipa possui um Chefe de Equipa, com um ou mais adjuntos que assumem autoridade na ausência deste. O Chefe de Equipa é responsável por (NIST, 2012, p. 16):

- Atuar como elo de ligação com a estrutura superior de gestão da organização e outras equipas e organizações;
- Desativar situações de crise;
- Assegurar que a equipa tem o pessoal, os recursos e as competências necessárias;
- Assegurar que as atividades de resposta a incidentes são executadas corretamente.

Algumas equipas possuem ainda o Líder Técnico (LT), com elevadas competências técnicas e experiência de resposta a incidentes. É ele que assume a supervisão e a responsabilidade final pela qualidade do trabalho técnico da equipa (NIST, 2012, p. 16).

As equipas de maior efetivo possuem um Líder de Incidente (LI), sendo ele o POC principal para lidar com um incidente específico, responsável pelo tratamento do incidente. Cabe-lhe a si coordenar as atividades dos elementos que tratam o incidente, recolher informações destes elementos, fornecer atualizações de incidentes a outros grupos e assegurar que as necessidades da equipa são satisfeitas (NIST, 2012, p. 16).

Os membros da equipa de resposta devem ter excelentes competências técnicas, tais como: administração de sistemas e redes, programação, apoio técnico e deteção de intrusão. Devem ter uma boa capacidade de resolução de problemas, um pensamento crítico e saber trabalhar em equipa, pelas necessidades de cooperação e coordenação para o sucesso da resposta. A capacidade de comunicação e de escrita são importantes, pela necessidade de interagir com uma grande variedade de pessoas e para a elaboração de propostas e procedimentos. Não sendo necessário cada membro da equipa ser um perito técnico, deve haver pelo menos um elemento proficiente em cada área de tecnologia. É também útil, se alguns membros da equipa forem especializados em áreas técnicas específicas, tais como,

na deteção de intrusão de rede, análise de *malware* ou forense. Temporariamente, é útil trazer especialistas técnicos que não pertencem à equipa (NIST, 2012, pp. 16-17).

Existem outros grupos dentro da organização, que podem ter a necessidade de participar no tratamento do incidente, como (NIST, 2012, pp. 17-18):

- A gerência superior/direção, para estabelecer a política de resposta, o orçamento e o pessoal. É responsável pela coordenação da resposta entre as várias partes interessadas, minimizar os danos e informar as outras partes.
- O pessoal de segurança da informação, pode ser necessário durante certas fases de tratamento de incidentes (prevenção, contenção, erradicação e recuperação) (p. ex. para alterar a rede de controlos de segurança).
- Os técnicos das TI (p. ex. os administradores de sistemas e de redes) pelas suas competências, para prestar o apoio e pela melhor compreensão da tecnologia que gerem numa base diária, permitindo assegurar que sejam tomadas as medidas apropriadas para o sistema afetado.
- Os peritos jurídicos, para reverem os planos de resposta, as políticas e os procedimentos, assegurando a sua conformidade com a lei (incluindo o direito à privacidade). Deve-se ainda, recorrer a estes especialistas sempre que se avalie a possibilidade de um incidente ter ramificações legais, incluindo a recolha de provas; a acusação de um suspeito; uma ação judicial; a necessidade de um memorando de entendimento, ou outro acordo vinculativo que envolva limitações de responsabilidade para partilha de informação.
- As relações públicas com os media, consoante a natureza e impacto de um incidente, pode existir a necessidade de informar os meios de comunicação social e o público.
- Os Recursos humanos (p. ex. para efeitos disciplinares, caso um funcionário seja suspeito de causar um incidente).
- Os profissionais pelo planeamento da continuidade do negócio. Estes elementos têm de ter conhecimento do impacto dos incidentes, de modo a poderem efetuar as avaliações de impacto empresarial, as avaliações do risco e a continuidade dos planos de operações. Pela sua experiência em minimizar a disrupção operacional, o seu apoio pode fazer a diferença no planeamento da resposta a adotar, em determinadas situações (p. ex. em condições de negação de serviços).

- Os responsáveis pela segurança física e gestão de instalações, para permitir o acesso às instalações durante o tratamento de incidentes (p. ex. acesso a uma estação de trabalho comprometida a partir de um escritório fechado à chave).

4.1 Síntese conclusiva

O **processo** de reação a incidentes do NIST é composto por 4 fases, sequenciais e cíclicas: preparação; deteção e análise; contenção, erradicação e recuperação; e pós atividade do incidente.

Como **entidades** primárias para a resposta a incidentes, identificam-se as CSIRT, apoiadas por outras entidades, internas e externas, da organização.

As entidades internas (em apoio) podem ser a gerência superior/direção, o pessoal da segurança da informação, os elementos da segurança física e gestão de instalações, os técnicos das TI, o LEGAD, o departamento de assuntos públicos, os recursos humanos e os profissionais pelo planeamento da continuidade do negócio.

As entidades externas (em apoio) podem ser o CSIRT Nacional, outros CSIRT, Forças de Segurança, entidades com conhecimento especializado, outras organizações, media e os clientes.

O **modelo estrutural** da CSIRT pode ser: Equipa de Resposta a Incidentes Central, Equipa de Resposta a Incidentes Distribuída ou Equipa de Coordenação.

A Equipa pode ser composta segundo 3 modelos: Funcionários (toda a organização realiza todo o seu trabalho de resposta); Parcialmente *Outsourced* (organização subcontrata pessoal para executar parte do trabalho de resposta); e Totalmente *Outsourced* (a organização subcontrata todo o seu trabalho de resposta). Nos modelos Funcionários e Parcialmente *Outsourced* as equipas são constituídas pelo Chefe Equipa, Adjuntos, LT, LI e Membros da Equipa. No modelo Totalmente *Outsourced*, a equipa é constituída pelo Supervisor e 1 ou 2 reservas.

As responsabilidades das entidades referidas anteriormente, encontram-se sistematizadas no quadro do Apêndice E e na figura seguinte.

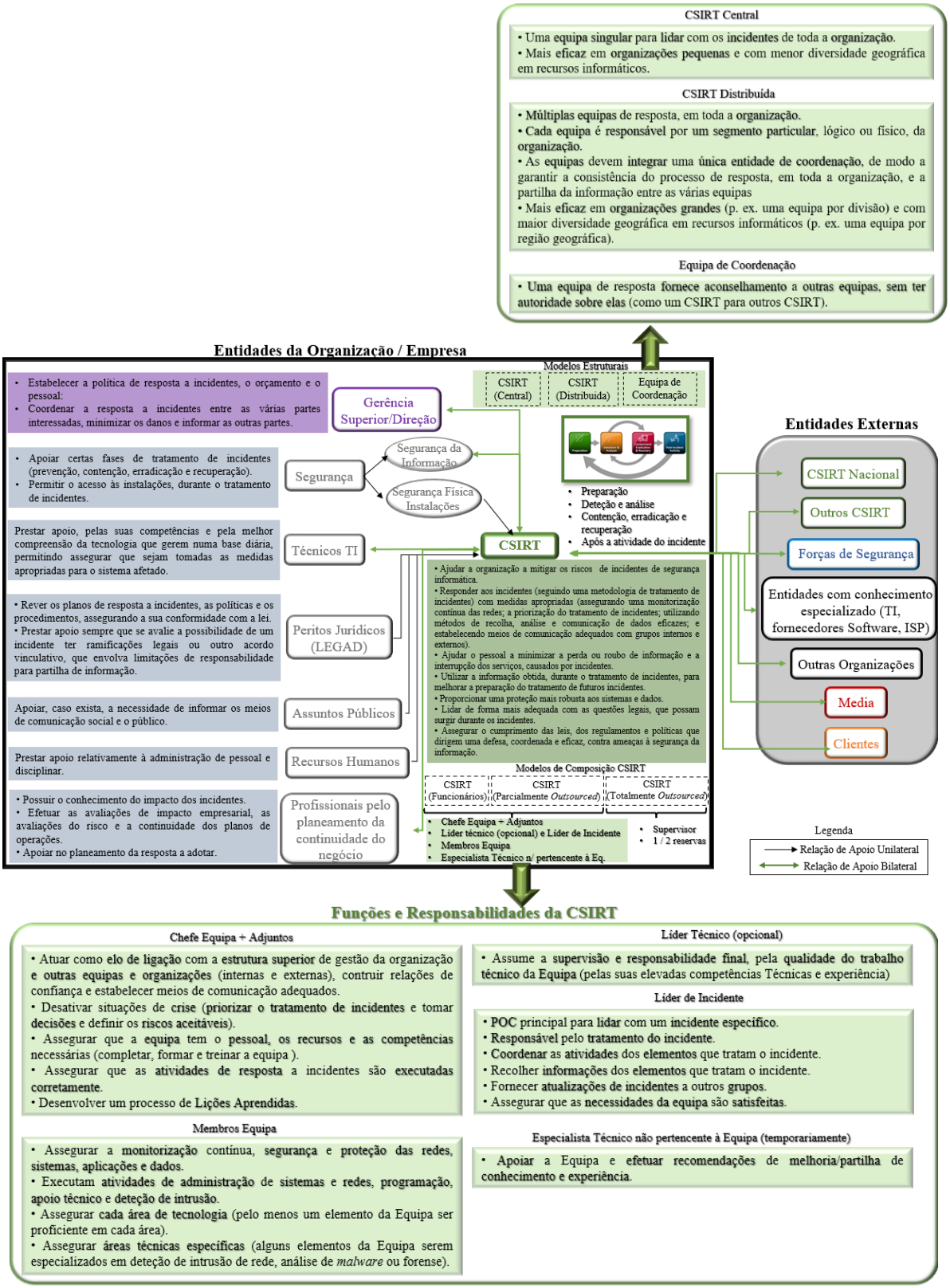


Figura 4 - Estrutura, processos e responsabilidades existentes no NIST, na resposta a ciberincidentes

Fonte: Adaptado a partir de NIST (2012).

Assim, considera-se respondida **QD1, qual a estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes?**

5. Adequabilidade da estrutura, processos e responsabilidades previstos na lei orgânica do EMGFA (2022), na escalada de resposta a ciberincidentes

Neste capítulo, efetua-se uma análise da nova organização das FFAA para verificar a adequabilidade da sua estrutura, processos e responsabilidades na escalada da resposta a ciberincidentes, comparativamente ao NIST, identificando-se possíveis lacunas existentes no modelo da organização atual.

Tendo em conta o enquadramento relativo à Lei Orgânica (2022) do EMGFA apresentado no Apêndice F, o gabinete do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), entre outras, compreende a Assessoria Jurídica (para prestar apoio jurídico e contencioso e conduzir os assuntos de natureza jurídica, no âmbito das atribuições e competências do EMGFA) e as Relações Públicas (para assegurar as atividades de comunicação, informação e relações públicas do EMGFA) (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 10).

O Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE) dispõe de autoridade técnica no âmbito das Comunicações e Sistemas de Informação (CSI), guerra eletrónica, e segurança da informação (SegInf); e dispõe de autoridade funcional e técnica no âmbito da ciberdefesa. Das suas atribuições (Apêndice G), realça-se a sua responsabilidade na condução da resposta a incidentes; no conhecimento situacional do ciberespaço; na partilha de informação; na cooperação com outras entidades nacionais de cibersegurança; e no desenvolvimento de capacidades de prevenção, monitorização, deteção, reação, análise e correção de ciberincidentes (Decreto-Lei n.º 19/2022, de 24 de janeiro, pp. 4 e 22-23).

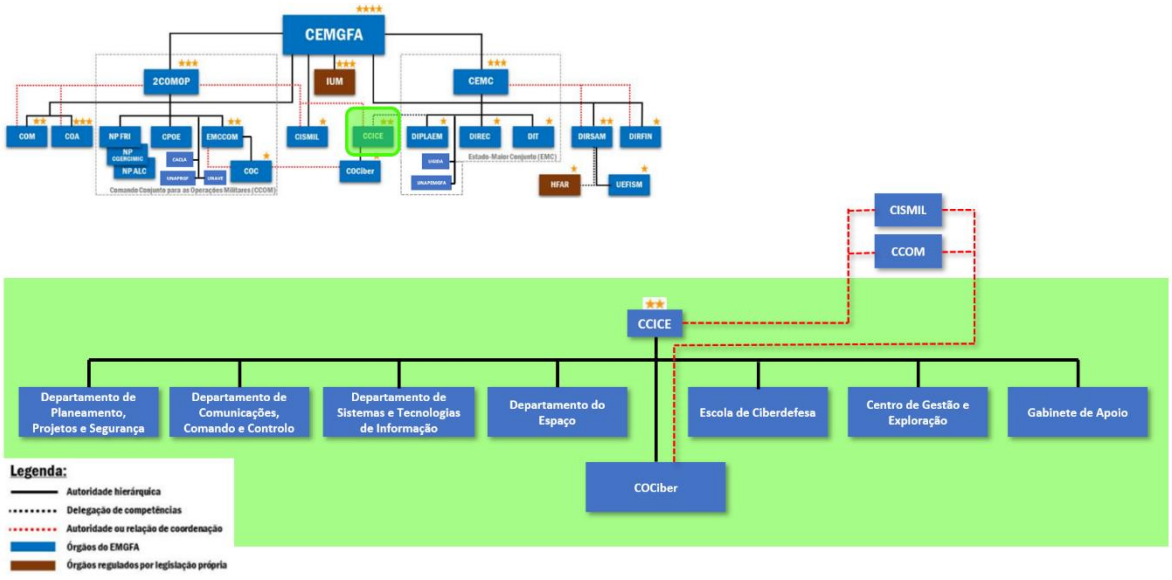


Figura 5 - Macroestrutura do CCICE

Fonte: Adaptado a partir de Decreto-Lei n.º 19/2022, de 24 de janeiro (p. 23).

5.1 Capacidade de resposta a ciberincidentes no EMGFA/COCiber

O COCiber, sob a direta dependência do Chefe do CCICE, passa a deter a responsabilidade de "planear, dirigir, coordenar, controlar e executar operações no e através do ciberespaço em apoio a objetivos militares, garantindo a liberdade de ação das FFAA neste domínio" (Decreto-Lei n.º 19/2022, de 24 de janeiro, pp. 23-24). Das suas atribuições (Apêndice G), enquadradas pelas do CCICE, destaca-se a condução de operações no ciberespaço ao nível tático e operacional; ser o único ponto de contato das FFAA para a ciberdefesa nacional; assegurar o conhecimento situacional; planear soluções para a proteção da informação e sistemas de informação; colaborar na investigação, recolha e salvaguarda de prova no processo de análise de incidentes nas redes da Defesa Nacional (DN); cooperar com as estruturas nacionais de cibersegurança; e partilhar informação com os CIRC nacionais e internacionais e com o CNCS.

O COCiber detém autoridade de coordenação com o Comando Conjunto para as Operações Militares (CCOM) e o Centro de Informações e Segurança Militares (CISMIL), no âmbito do planeamento e da condução de operações militares. Relaciona-se também, diretamente, com as estruturas internacionais ligadas à ciberdefesa e à cibersegurança cooperativa, nomeadamente da OTAN e União Europeia (Decreto-Lei n.º 19/2022, de 24 de janeiro, pp. 4, 23-25).

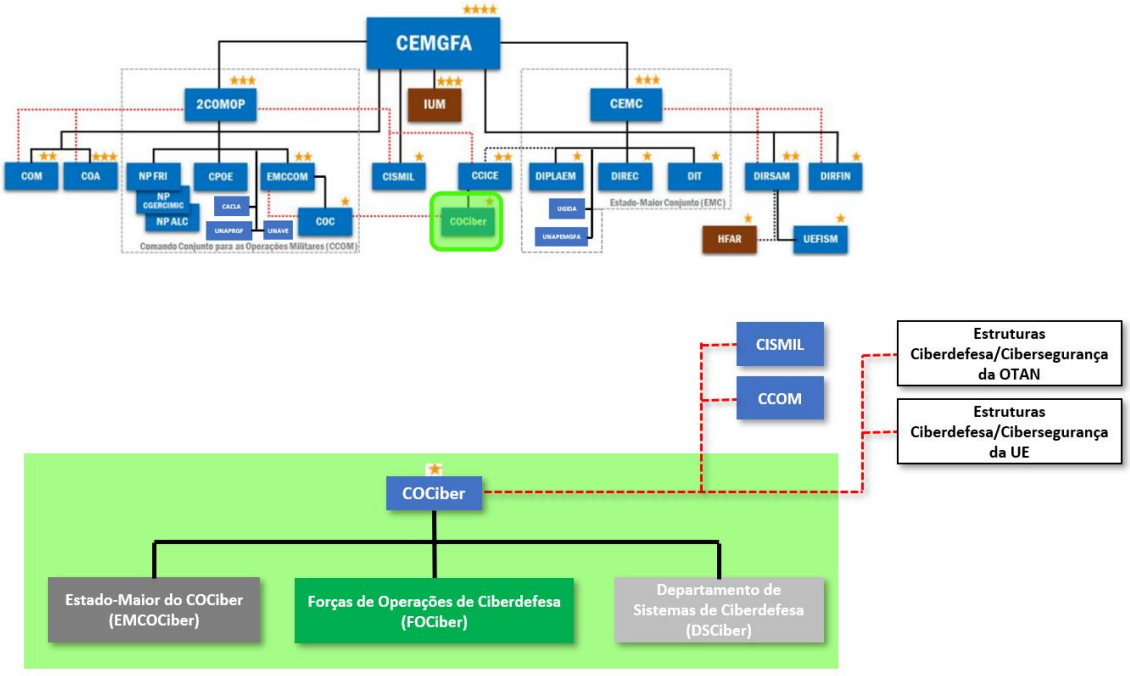


Figura 6 - Macroestrutura do COCiber

Fonte: Adaptado a partir de Decreto-Lei n.º 19/2022, de 24 de janeiro (p. 24).

O COCiber tem na sua dependência técnica e funcional o Núcleo CIRC (NCIRC) do EMGFA e as componentes de ciberdefesa dos Ramos. Tem autoridade técnica com o NCIRC do Ministério da Defesa Nacional (MDN) e o Centro de Dados da Defesa (CDD) (EMGFA, 2021, p. 2).

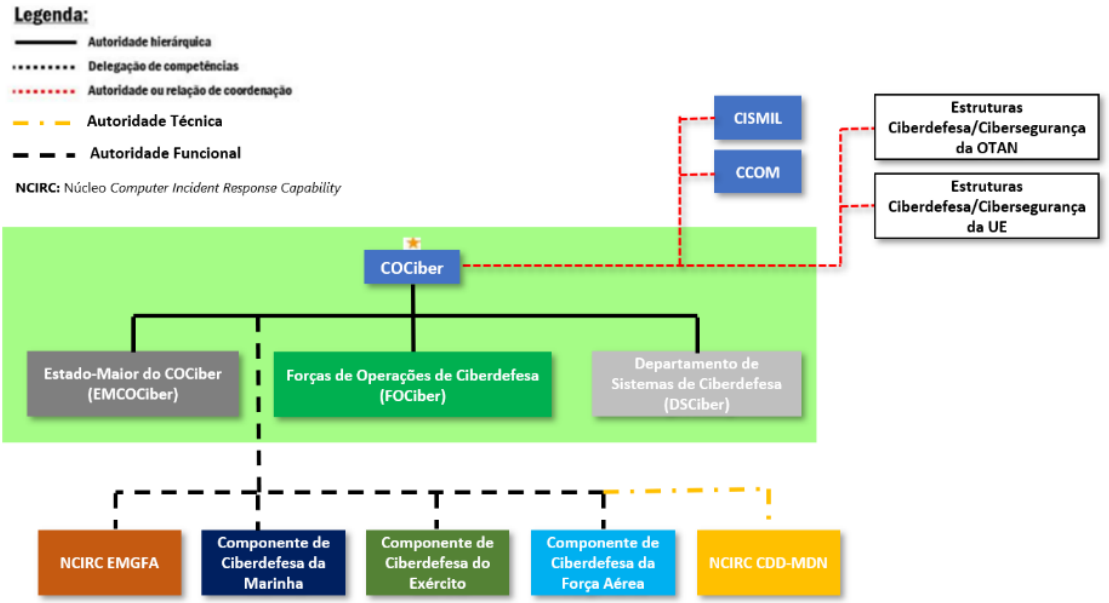


Figura 7 - Microestrutura do COCiber, dependências funcionais e técnicas

Fonte: Adaptado a partir de EMGFA (2021, p. 2).

Das várias entidades que compõem o Estado-Maior (EM) do COCiber (EMCOCiber), equiparadas às do NIST, salientam-se (indicando algumas das suas responsabilidades) (EMGFA, 2021, pp. 4-15):

- Na C0 (Coordenação), a célula responsável pela assessoria jurídica ao COCiber, incumbida dos atos legislativos e regulamentos administrativos relativos ao funcionamento e organização da ciberdefesa nas FFAA; assegurar o apoio jurídico ao COCiber e às operações; o enquadramento legal na resposta aos incidentes e ações no ciberespaço; a inserção nas Regras de Empenhamento de aspetos legais; os memorandos de entendimento e outros contratos assegurando a sua adequação à missão e às operações militares no ciberespaço; a avaliação da eficácia e eficiência das leis, regulamentos e políticas aplicadas ao ciberespaço.

- Na C2 (Informações), o Núcleo de Conhecimento Situacional, o Núcleo de Análise de Informações e o Núcleo de Contrainformação e Interagências de Informações responsáveis, respetivamente, por disponibilizar uma perceção dos atores e ameaças relevantes no ciberespaço de interesse nacional conjuntural (o conhecimento situacional do ciberespaço); identificar ameaças, atores e motivações de forma a permitir o planeamento e execução de operações que permitam reduzir, mitigar o risco ou as ameaças efetivas, particularmente, determinar e realizar uma análise interna e externa das potenciais ameaças, investigando todos os indicadores relativos a ataques no ciberespaço; analisar, processar e disseminar as informações recolhidas pela Forças de Operações de Ciberdefesa (FOCiber) e recebidas pelo COCiber (de outras agências de informações); manter a ligação às agências de informações nacionais e internacionais, e coordenar os assuntos relacionados com informações militares e contrainformação no ciberespaço com as entidades externas às FFAA.
- Na C3 (Operações), o Núcleo de Operações Correntes responsável pela condução, controlo e coordenação das operações militares no ciberespaço, empregando de forma eficiente os recursos; avaliar o sucesso da operação e o impacto dos efeitos provocados; coordenar os esforços de mitigação com os responsáveis dos sistemas; e manter atualizado o conhecimento situacional das operações.
- Na C5 (Planos), o Núcleo de Planeamento responsável por apoiar o processo de tomada de decisão do Comandante durante uma operação; elaborar estudos, planos, informações, pareceres ou propostas no âmbito da edificação de capacidades, organização operacional e geração de forças; e manter a matriz de risco atualizada.
- Na C7 (Formação e Treino), o Núcleo de Formação e o Núcleo de LA responsáveis, respetivamente, pelo planeamento e acompanhamento da execução dos planos de formação, qualificação e treino dos recursos humanos; e aplicar os procedimentos da OTAN de LA.
- Na C9 (Cooperação e Relações Externas), o Núcleo de Relações Interagências responsável por assegurar a coordenação e cooperação interagências, no âmbito de assuntos expressamente associados ao ciberespaço, com o CNCS e

o CERT Portugal (CERT.PT - uma organização liderada pelo CNCS que reúne todos os CERT nacionais); e a coordenação de atividades e representação do COCiber no fórum Grupo 4 (grupo para coordenação e partilha de informações relativas à segurança do ciberespaço, constituído pelo COCiber, CNCS, Polícia Judiciária – PJ – e o Serviço de Informações de Segurança – SIS), CERT.PT e com outros organismos nacionais com competências no ciberespaço.

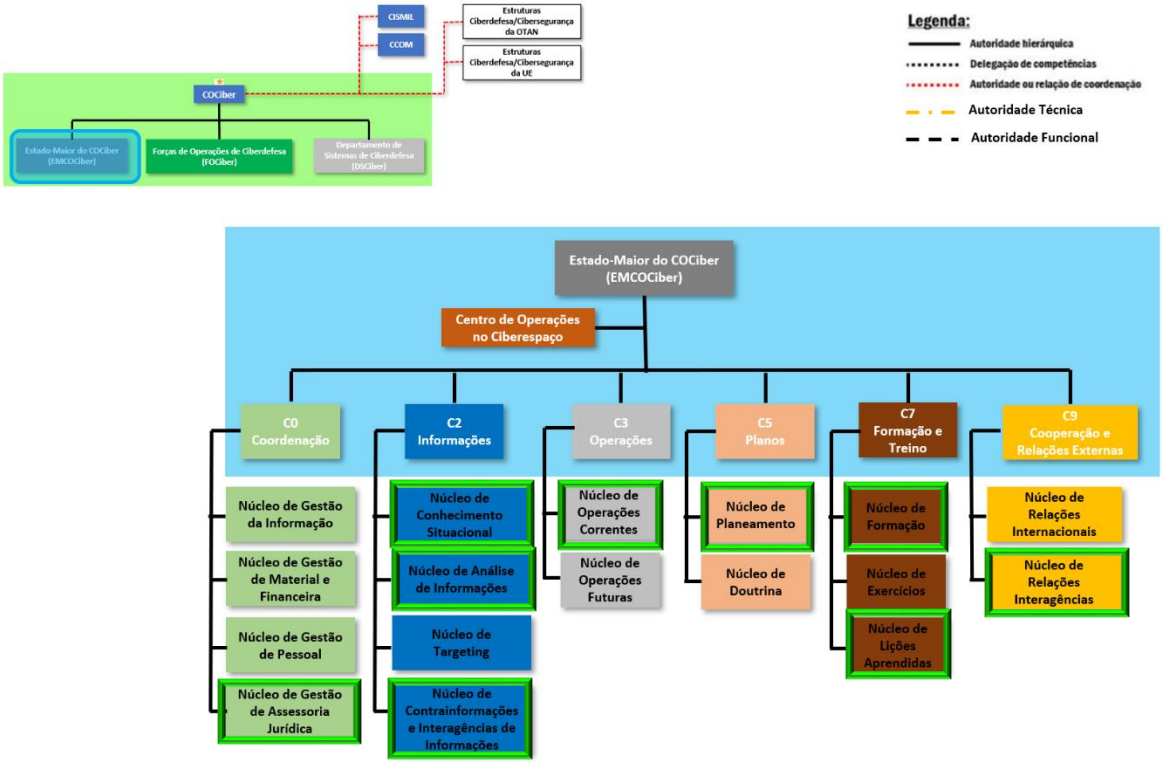


Figura 8 - Macroestrutura do EMCOCiber

Fonte: Adaptado a partir de EMGFA (2021, p. 5).

O Centro de Operações no Ciberespaço (OPSCiber) é onde se efetua o planeamento, preparação, controlo, coordenação, condução e a avaliação das operações militares no ciberespaço. Este centro é guarnecido por elementos do EMCOCiber (EMGFA, 2021, p. 23).

As funções desempenhadas no OPSCiber são (EMGFA, 2021, pp. 23-24):

- Diretor do OPSCiber, desempenhado pelo Chefe da C3, responsável pela organização e operação do OPSCIber.
- *Battle Watch Captain* (BWC), desempenhado pelos Oficiais da C3 e C5, responsável pela coordenação do OPSCiber; por manter o conhecimento

situacional; conduzir, coordenar e sincronizar as operações militares; e reagir a qualquer situação emergente ou incidente.

- Adjunto do *Battle Watch Captain* (ABWC), desempenhado pelos Sargentos da C3 e C5, responsável pelos registos e gestão do pessoal de serviço ao OPSCiber.
- *Intel Watchkeeper* (IWC), desempenhado pelos Oficiais da C2, responsável por manter atualizado o panorama situacional das informações e a matriz de risco das operações; analisar e disseminar a informação recebida das diversas fontes.
- Consoante as necessidades, outras funções podem ser ativadas.

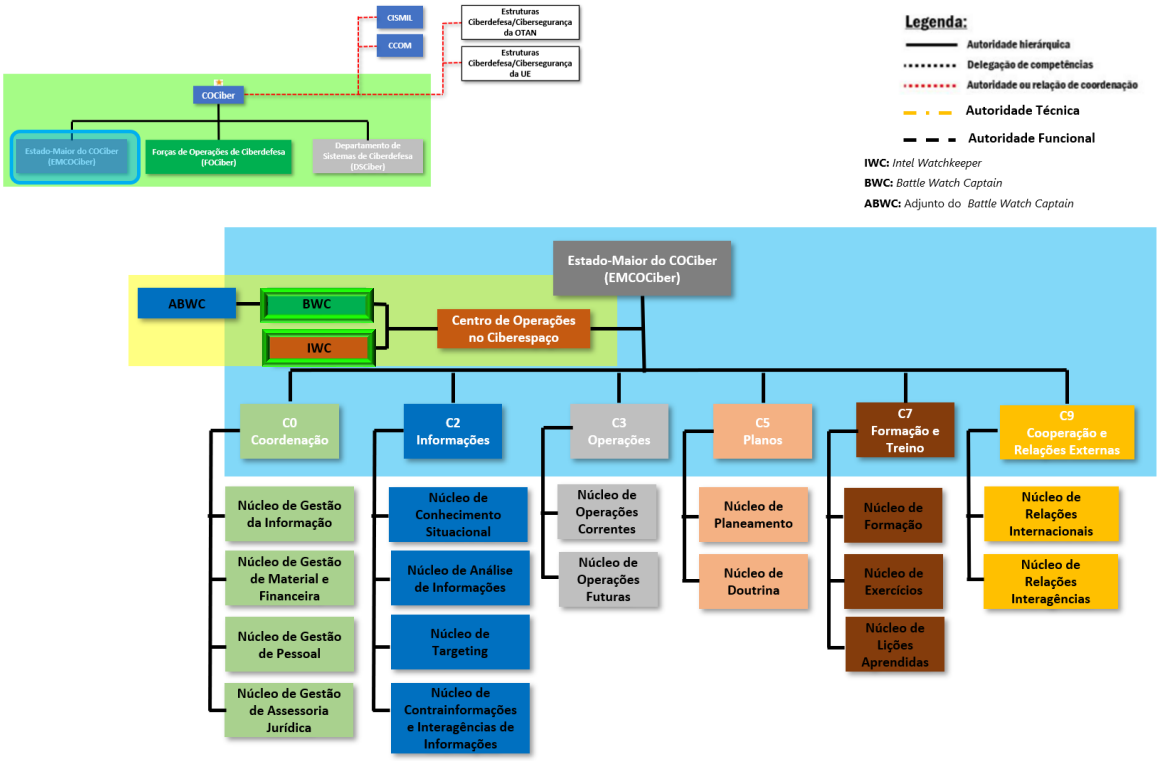


Figura 9 - Macroestrutura do OPSCiber

Fonte: Adaptado a partir de EMGFA (2021, p. 23).

As FOCiber garantem a execução de operações defensivas nos sistemas e redes da DN (e em outras à sua responsabilidade); operações de exploração, vigilância e reconhecimento; e operações ofensivas no e através do ciberespaço. Cabe a este órgão, entre outras atribuições, garantir a componente e suporte técnico às operações no ciberespaço; aconselhar o comando superior das soluções técnicas mais adequadas para cumprir os objetivos; e garantir a constituição das Equipas das Forças de Missão do Ciberespaço (EFMCiber) de acordo com as missões atribuídas (EMGFA, 2021, p. 15).

De destacar as entidades que compõem as FOCiber, equiparadas às do NIST (EMGFA, 2021, pp. 16-18):

- Da Secção de Informações Táticas, o Núcleo de conhecimento Situacional e o Núcleo de Exploração responsáveis por, respetivamente, desenvolver sob a coordenação da C2 a atividade de informações, vigilância e reconhecimento (ISR); e utilizar provas de ataques anteriores e indicadores de comprometimento para identificar e classificar possíveis ataques futuros.
- A Secção de Defesa, responsável por garantir a operação das plataformas de monitorização em produção na Defesa; contribuir para o esclarecimento situacional das atividades no ciberespaço das redes da Defesa; estabelecer a ligação com a os núcleos CIRC da Defesa (dos Ramos) e coordenar a resposta a incidentes.
- A Secção de Resposta, responsável por executar ações de resposta a eventos de segurança nas redes da Defesa; enquanto especialistas em ciberdefesa/cibersegurança, participar em projetos de investigação e desenvolvimento (I&D); e analisar vulnerabilidades.
- A Secção de Investigação Digital, responsável por efetuar perícias digitais especializadas e de engenharia inversa de análise forense digital; e apoiar projetos de I&D, enquanto especialistas na área da análise forense digital.

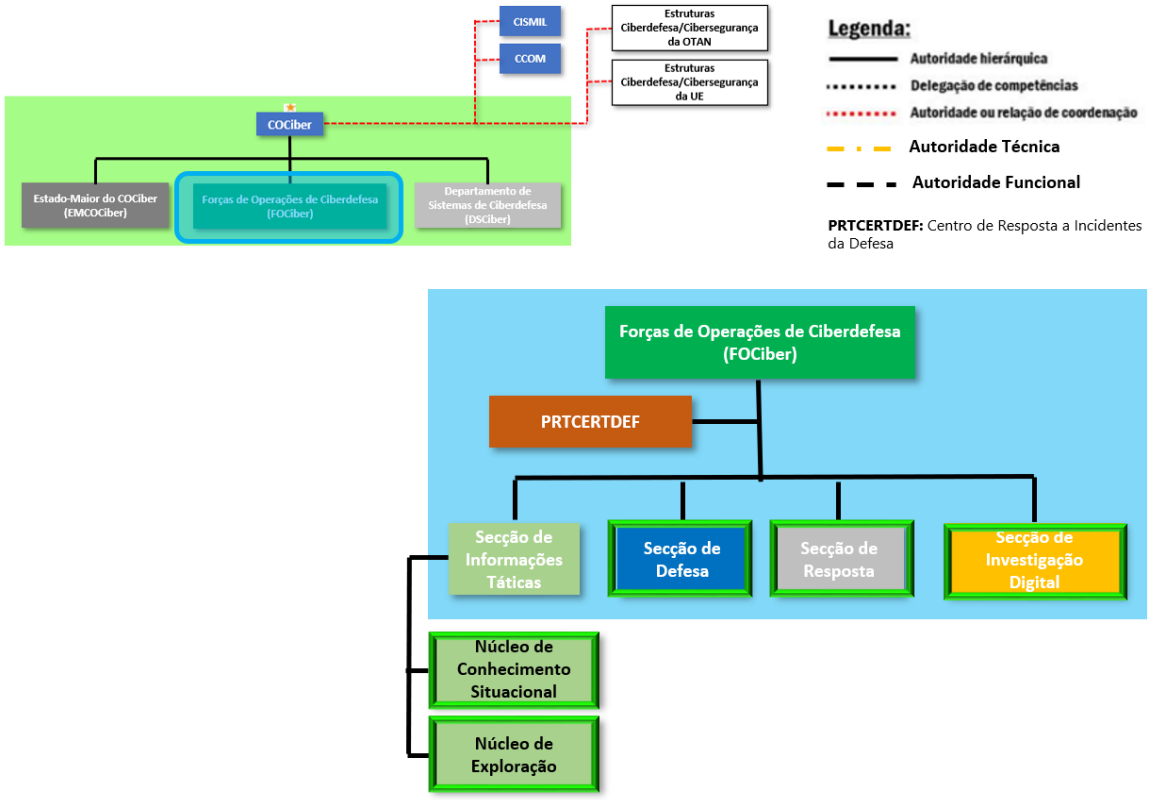


Figura 10 - Macroestrutura das FOCiber

Fonte: Adaptado a partir de EMGFA (2021, p. 16).

São as FOCiber, sob a coordenação do Chefe da FOCiber, que guarnecem o centro de resposta a incidentes no ciberespaço da DN (PRTCERTDEF), onde é efetuada a direção técnica, monitorização e coordenação da resposta a incidentes das redes da DN (as CERT da Defesa) (EMGFA, 2021, pp. 15 e 25).

Os órgãos e entidades que compõem o PRTCERTDEF, são os seguintes (EMGFA, 2021, pp. 25-26):

- Chefe de Divisão ao PRTCERTDEF, guarnecido pelos Oficiais Superiores, Capitães e Subalternos das FOCiber, responsável por definir as prioridades de execução e garantir a ativação das células necessárias para o cumprimento das tarefas definidas superiormente.
- Célula de *Intel*, guarnecida por elementos da Secção de Informações Táticas, responsável por manter a vigilância permanente das fontes de *Intel*, mantendo informado o Chefe de Divisão do PRTCERTDEF e os elementos da célula de Vigilância e Deteção sobre informações relevantes.

- Célula de Vigilância e Deteção, guarnecida por elementos das Secções de Defesa e de Resposta, responsável por manter a vigilância permanente nas redes da defesa, reagindo aos eventos anómalos.
- Célula de Análise Forense, guarnecida por elementos da Secção de Análise Forense, responsável por realizar investigações forenses aos eventos anómalos.
- Célula de Reconhecimento e Antecipação, guarnecida por elementos do Núcleo de Exploração, responsável pelo reconhecimento de sistemas ou redes digitais e pela execução de medidas preventivas de proteção dos sistemas da Defesa ou penetração de alvos.
- Célula de Resposta e Apoio Técnico ao Planeamento, guarnecida por elementos da Secção de Resposta, responsável por executar a resposta a eventos (e ações ofensivas se determinado superiormente); garantir o aconselhamento técnico no processo de planeamento e elaborar os planos técnicos para provocar os efeitos desejados.

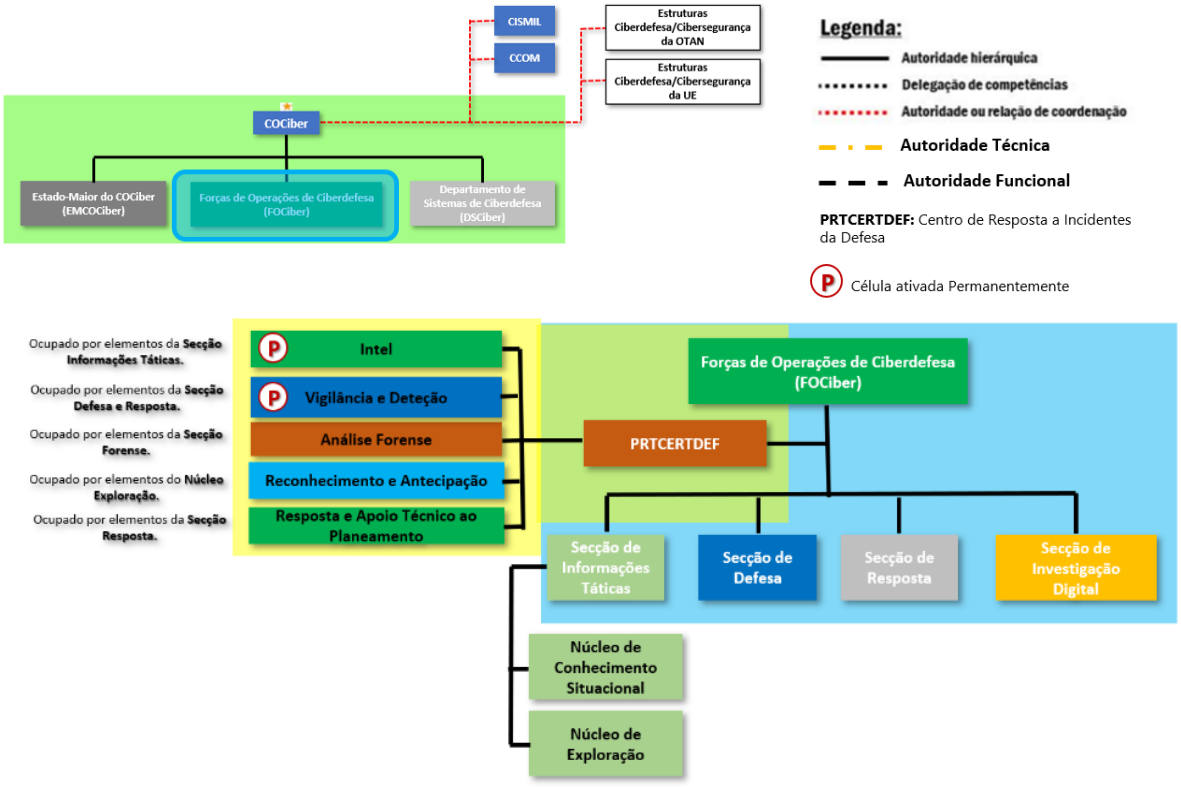


Figura 11 - Macroestrutura do PRTCERTDEF

Fonte: Adaptado a partir de EMGFA (2021, p. 25).

O Departamento de Sistemas de Ciberdefesa (DSCiber) tem a missão de planear e edificar a infraestrutura tecnológica; definir os requisitos para obter e garantir a sustentação dos meios, plataformas e sistemas de ciberdefesa e assegurar a interoperabilidade com os parceiros, aliados, nações amigas e organizações internacionais. É responsável pela realização de auditorias de vulnerabilidades nas redes e sistemas de informação e comunicações das FFAA, permitindo uma melhor gestão do risco, e pelo apoio e assessoria técnica ao COCiber. Das suas várias competências, salientam-se, garantir a operacionalidade da infraestrutura e o apoio técnico às operações no ciberespaço, do COCiber, do OPSCiber, do PRTCERTDEF e das áreas de ciberdefesa dos Ramos; definição e implementação de soluções tecnológicas de segurança; participar com o EMGFA e os Ramos na *Federated Mission Networking*, ou iniciativas similares, que visem a agilidade, flexibilidade e escalabilidade nas missões no ciberespaço (EMGFA, 2021, pp. 18-19).

Das várias entidades que compõem as DSCiber, equiparadas às do NIST, salientam-se (EMGFA, 2021, pp. 19-22):

- A Secção de Tecnologias de Ciberdefesa, responsável por estabelecer e assegurar o cumprimento de um plano de mitigação e continuidade de operações; e assegurar a confidencialidade, integridade e disponibilidade da informação no COCiber.
- A Secção de Auditorias e Análise de Vulnerabilidades, responsável pela gestão do risco e de potenciais impactos nos sistemas das FFAA; e propor e avaliar medidas de resposta ao risco associadas às vulnerabilidades encontradas.

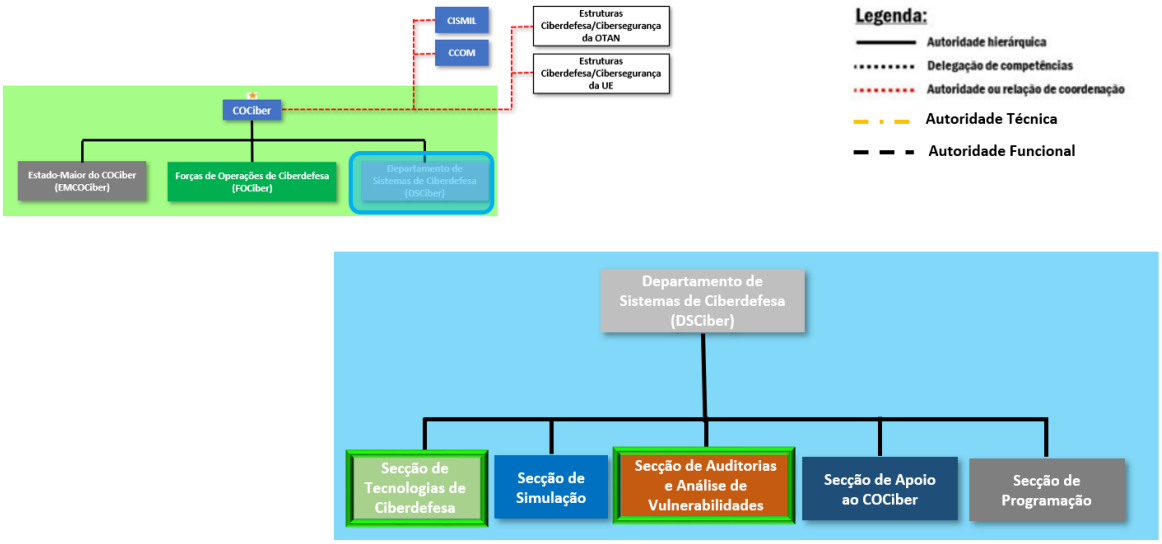


Figura 12 - Macroestrutura do DSCiber

Fonte: Adaptado a partir de EMGFA (2021, p. 19).

5.2 Capacidade de resposta a ciberincidentes no Exército

No Exército, é criada a Direção de Comunicações e Informação (DCI) (na dependência direta do Vice-Chefe do Estado-Maior do Exército) com o intuito de garantir a fluidez operacional, procedendo-se à centralização, entre outras, das áreas das CSI, da gestão da informação e do conhecimento, da ciberdefesa e da SegInf (Decreto-Lei n.º 19/2022, de 24 de janeiro, pp. 5 e 75).

Tendo esta direção assumido as funções da anterior Direção de Comunicações e Sistemas de Informação (DCSI), a capacidade de ciberdefesa do Exército é implementada através do Centro de Transmissões (CTms) da DCSI e do Núcleo CIRC do Exército (NuclCIRCEx) (Estado Maior do Exército [EME], 2017a, p. 3).

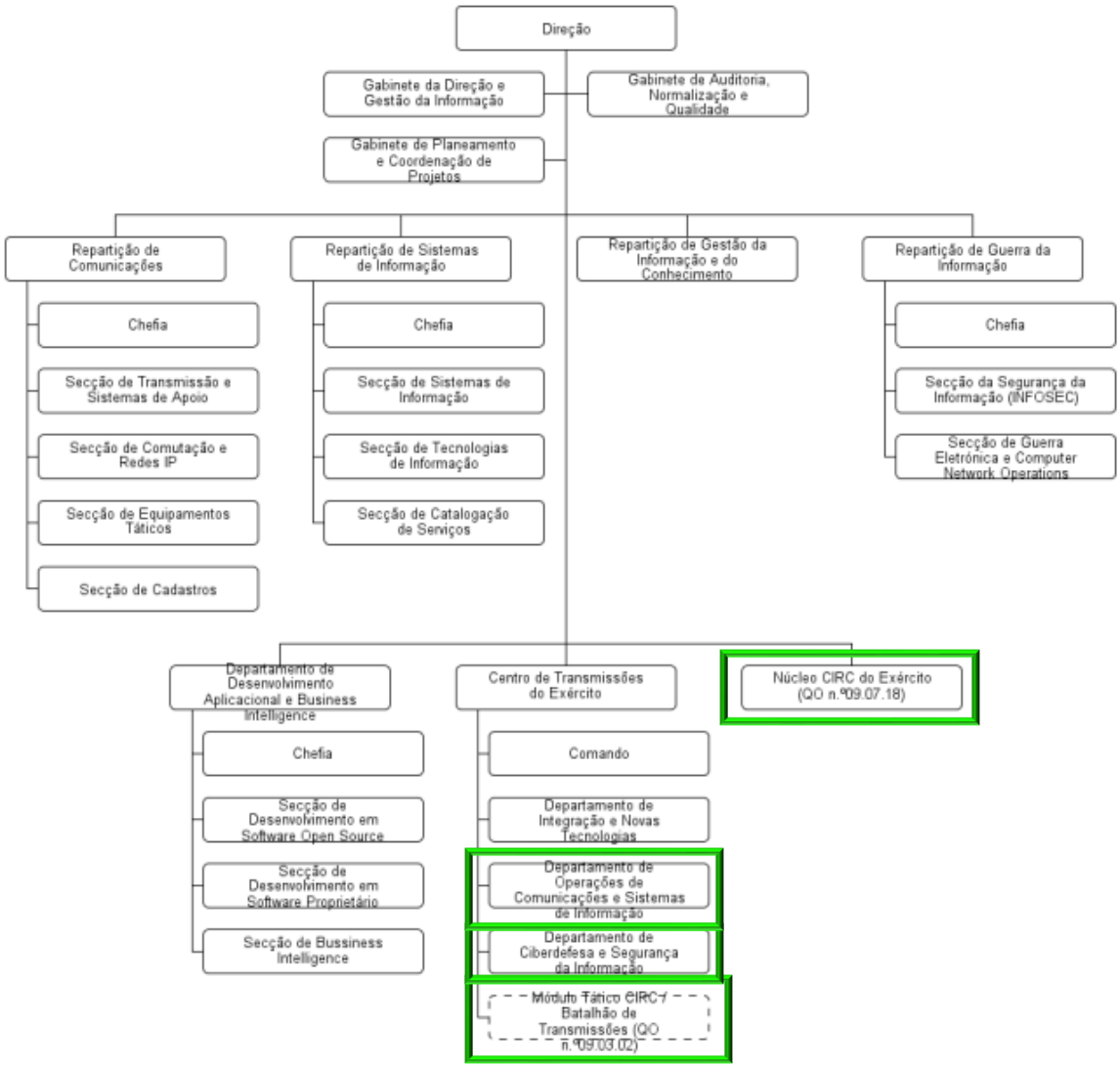


Figura 13 - Capacidade de ciberdefesa na estrutura da DCSI do Exército

Fonte: Adaptado a partir de EME (2017a, p. 3).

O CTms do Exército integra (EME, 2017a, pp. 15-17; EME, 2016, pp. 22 e 23):

- No Departamento de Operações de Comunicações e Sistemas de Informação, 01 Equipa CIRC do Destacamento de Comunicações e Sistemas de Informação do Centro (Centro de Controlo e Gestão Alternativo); 01 Equipa CIRC do Destacamento de Comunicações e Sistemas de Informação do Norte.
- No Departamento de Ciberdefesa e Segurança da Informação, o Comandante do Módulo Tático CIRC (ModTatCIRC) do Núcleo de Operações de Ciberdefesa (Oficial Adjunto deste núcleo).
- No ModTatCIRC do Batalhão de Transmissões (BTms – cujas atribuições estão no Apêndice G), 01 Seção Integradora, 01 Secção Ofensiva e 01 Secção Defensiva.

O ModTatCIRC, permite (EME, 2016, p. 5):

- Recolher e partilhar informações entre várias fontes e em tempo útil;
- Detetar incidentes/ataques, efetuar a avaliação de entidades e de situação;
- Prevenir, mitigar e por fim a um ciberataque;
- Efetuar a avaliação do risco para uma operação (no âmbito das CSI);
- Decidir as ações a implementar em tempo útil.

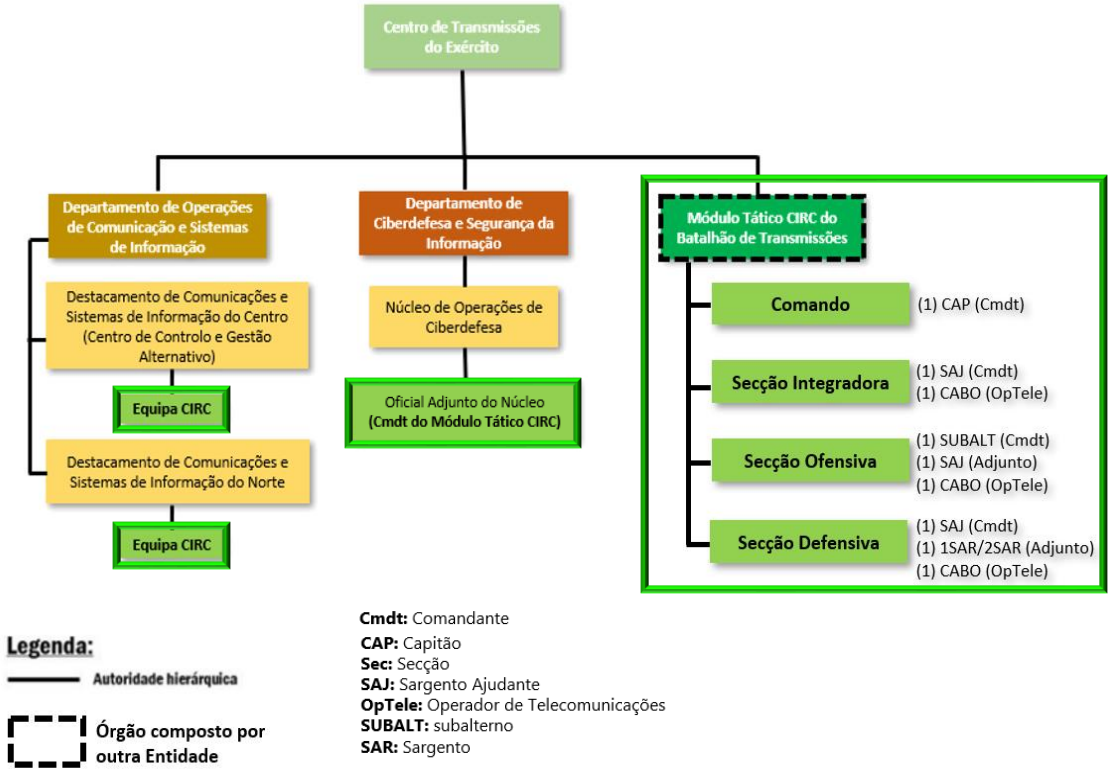


Figura 14 - Capacidade de ciberdefesa do CTms do Exército

Fonte: Adaptado a partir de EME (2017a, pp. 15-17; 2016, pp. 22-23).

O NuclCIRCEx está preparado para executar operações em todo o espectro das operações militares, no âmbito nacional ou internacional. Das suas possibilidades destacam-se (EMEb, 2017, p. 3):

- A capacidade de resposta a incidentes de segurança e defesa, do ciberespaço do Exército.
- A coordenação com o COCiber na resposta a incidentes de segurança, ao nível das FFAA.
- Trabalho colaborativo e integrado com os restantes Núcleos CIRC que integram a capacidade de ciberdefesa nacional.

Os seus efetivos (7 elementos) são provenientes da DCSI e, quando empregue operacionalmente, integra a estrutura do COCiber. Esta contempla (EMEb, 2017, pp. 3-5):

- Comando do Núcleo;
- 01 Secção de Resposta a Incidentes e Análise Forense (SecRespIncAnFor);
- 01 Secção de *Watchkeepers* e *Incident Handling Officers* (SecWatchkeepIncHandlOf).

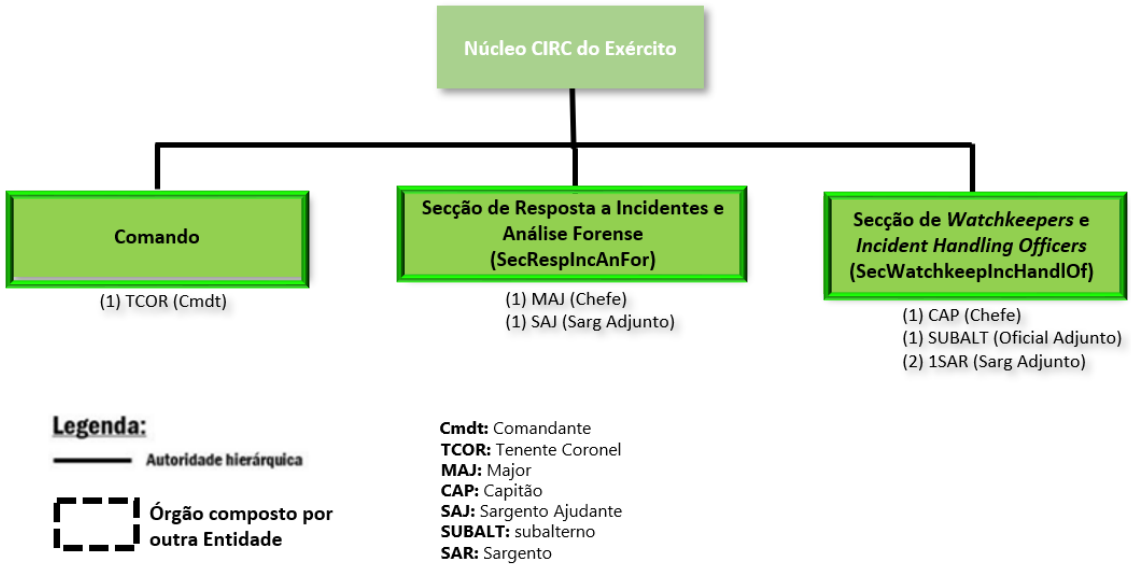


Figura 15 - Macroestrutura do NuclCIRCEx

Fonte: Adaptado a partir de EME (2017b, pp. 3-5).

5.3 Capacidade de resposta a ciberincidentes na Marinha

Na Marinha, a Superintendência da Informação compreende, entre outras, a Direção de Tecnologias de Informação e Comunicações (DITIC), incumbida de assegurar o exercício da autoridade técnica no domínio das CSI e Tecnologias de Informação e Comunicações (TIC) da Marinha. Entre as suas competências (Apêndice G), tem de assegurar a capacidade de resposta a incidentes e SegInf na Marinha, através de equipas próprias (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 61; Estado Maior da Armada [EMA], 2016, pp. 1-2).

Com capacidade de ciberdefesa, a DITIC tem na sua estrutura (EMA, 2016, pp. 4-5):

- O NCIRC.
- O Gabinete de Projetos, Normalização e Segurança (GPNS) que, em articulação com o NCIRC, é responsável por analisar o risco e propor medidas de mitigação de vulnerabilidades, dos equipamentos de segurança da infraestrutura TIC e CSI da Marinha. Tem na sua dependência a Equipa Técnica de Intervenção Rápida (ETIR).
- A ETIR, é uma equipa composta por técnicos de diferentes áreas tecnológicas (pertencentes à Divisão de Administração de Sistemas e de Comunicações – DAC – e à Divisão de Suporte aos Serviços e Sistemas em Exploração - DSE) permanentemente disponível, responsável por assegurar a capacidade de resposta adequada para a resolução de incidentes em áreas críticas, repondo os

sistemas e serviços que afetem a capacidade operacional ou as missões em curso. Articula-se, além do Oficial Coordenador da equipa, em 05 áreas técnicas (energia, *Military Message Handling System* – MMHS, redes, serviços e telecomunicações).

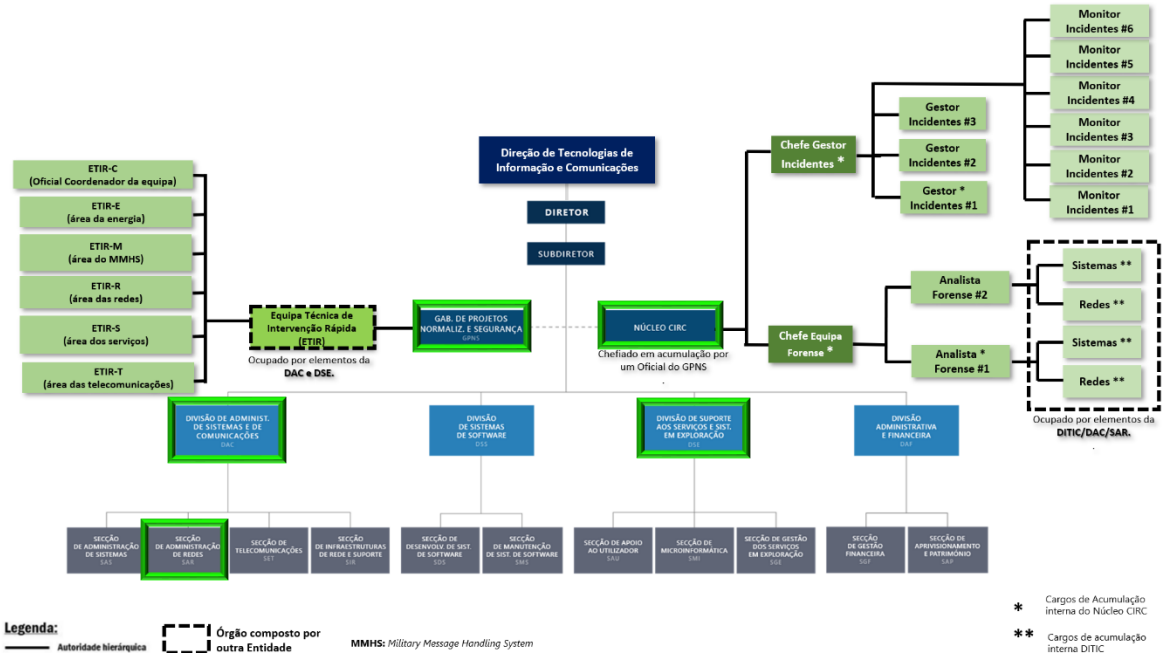


Figura 16 - Macroestrutura da DITIC, da Marinha

Fonte: Adaptado a partir de NCIRC da Marinha (Apresentação PowerPoint enviada por email, 20 de abril de 2023) e EMA (2016, pp. 4-5).

Das várias competências do NCIRC, salientam-se (EMA, 2016, p. 5):

- Garantir a capacidade de resposta a incidentes de segurança e defesa do ciberespaço e da informação.
- Assegurar a coordenação técnica da resposta a incidentes de SegInf.
- Assegurar a coordenação com o COCiber e com os NCIRC dos Ramos na resposta a incidentes de segurança, ao nível das FFAA ou infraestruturas críticas nacionais.
- O trabalho colaborativo e integrado com os restantes NCIRC da capacidade de ciberdefesa nacional.
- Partilhar informação com os NCIRC nacionais e internacionais.
- A gestão e tratamento de incidentes de SegInf, recolha de prova e realização de ações de investigação forense.

É chefiado por um oficial do GPNS (em acumulação), sob a direta dependência do Subdiretor de TIC, e em situações de resposta a incidentes é reforçado por técnicos das diferentes áreas tecnológicas. A sua estrutura contempla (EMA, 2016, p. 5; NCIRC da Marinha, Apresentação *PowerPoint* enviada por *email*, 20 de abril de 2023):

- O Chefe do NCIRC.
- 01 Equipa Forense, com 02 Analistas Forenses para as redes e sistemas.
- 01 Equipa de Gestão de Incidentes, com 03 Gestores de Incidentes e 06 Monitores de Incidentes.

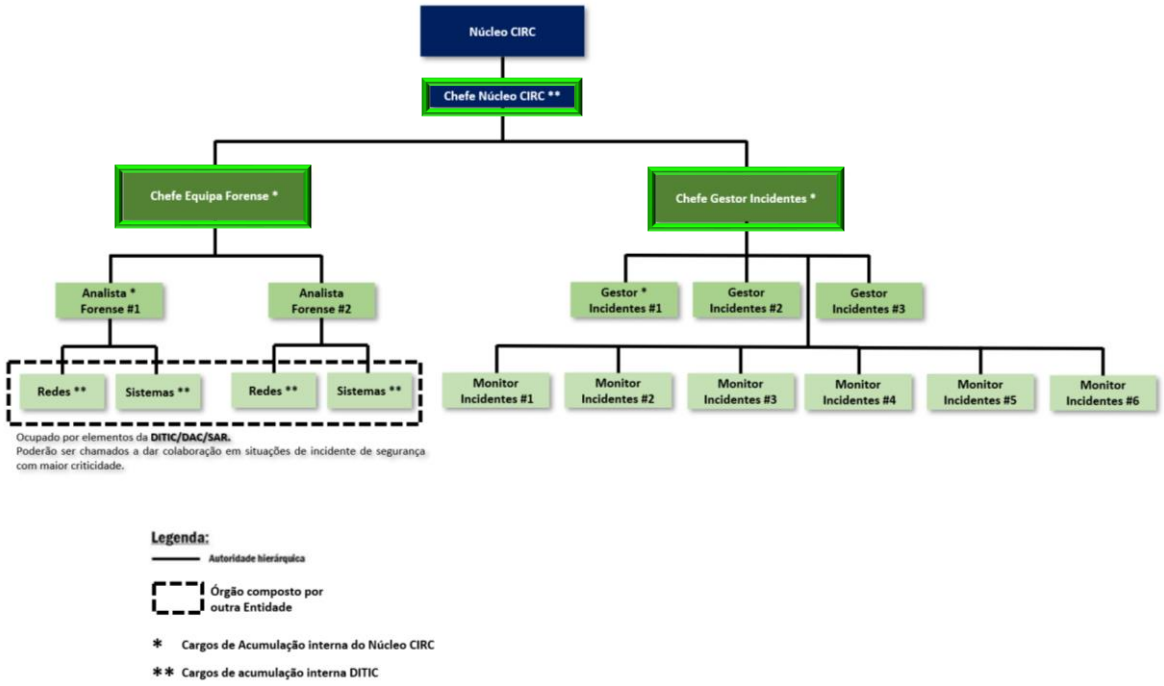


Figura 17 - Macroestrutura do NCIRC da Marinha

Fonte: Adaptado a partir de NCIRC da Marinha (Apresentação PowerPoint enviada por email, 20 de abril de 2023).

5.4 Capacidade de resposta a ciberincidentes na Força Aérea

Na Força Aérea (FA), a capacidade de ciberdefesa assenta em três níveis: o de Estado-Maior da Força Aérea (através da Divisão de Comunicações e Sistemas de Informação – DIVCSI), o de operação (através da DCSI do Comando da Logística da Força Aérea - CLAFA) e o de apoio (através dos Centros de Informática das Unidades). As suas competências (Apêndice G) realçam a necessidade de intervenção de grupos de resposta a incidentes e assegurar a confidencialidade, integridade e disponibilidade da informação (FA, 2011, pp. 4-3 e 4-4; FA, 2013, p. 6-2).

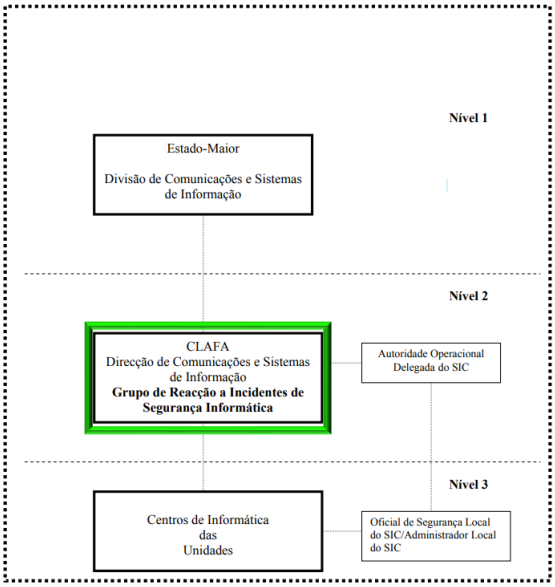


Figura 18 - A capacidade de ciberdefesa na FA

Fonte: Adaptado a partir de FA (2022, p. A-1).

A CIRT da FA, apesar de não estar assim identificada na documentação consultada, pelas funções dos elementos da Sub-Repartição de Segurança Informática e Ciberdefesa, é possível localizá-lo na Repartição de Tecnologias de Informação (RTI) da DCSI. Assim, poderemos interpretar que este CIRT tem a seguinte estrutura (FA, 2013, p. 6-2; Chefe de Estado Maior da Força Aérea [CEMFA], 2019, p. 281; CLFA, 2013, pp. 8-D-12 a 8-D-14):

- Chefe da Secção, responsável por dirigir, coordenar e controlar a execução das tarefas; e estabelecer normas e procedimentos de segurança dos Sistemas de Informação/Tecnologias de Informação (SI/TIC).
- Analistas de Segurança de SI/TIC, responsáveis por elaborar as normas técnicas de administração da infraestrutura tecnológica; implementação e monitorização das normas e medidas de segurança; monitorização dos sistemas de defesa de perímetro e segurança da rede em geral; colaborar na identificação e avaliação de soluções técnicas; colaborar na análise forense de incidentes informáticos e assegurar a capacidade de resposta a incidentes.

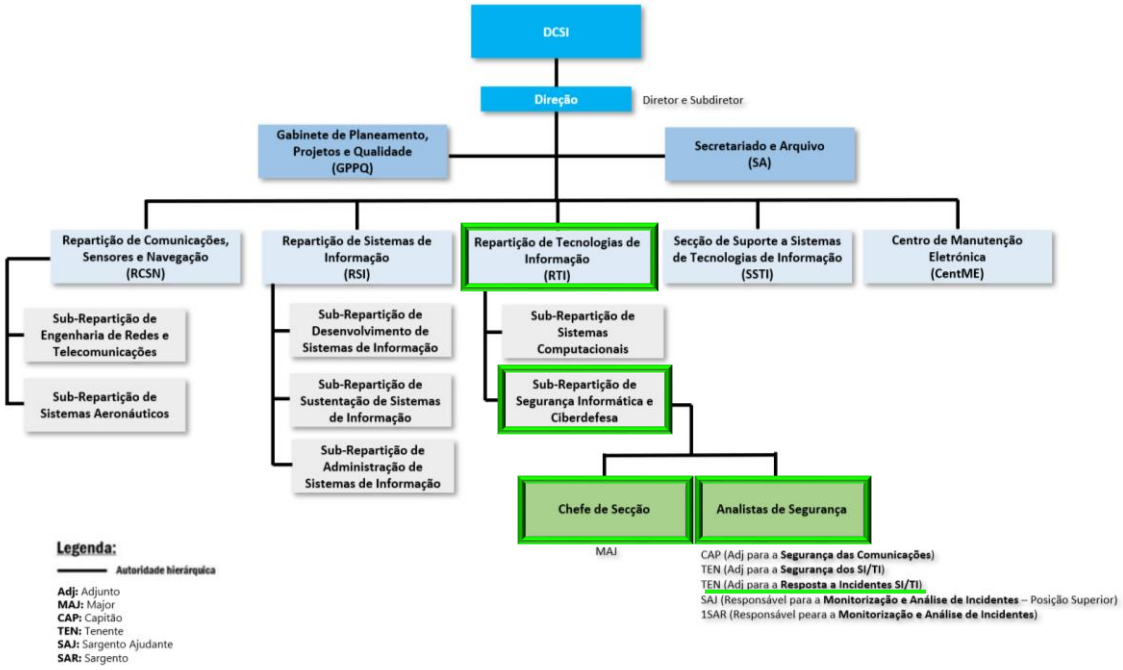


Figura 19 - Macroestrutura da DCSI da FA

Fonte: Adaptado a partir de FA (2013, p. 8-4), CEMFA (2019, p. 281).

5.5 Síntese Conclusiva

A partir da descrição anteriormente feita, foi elaborado o quadro que se apresenta no Apêndice H, com base nos indicadores em estudo, e que de seguida se procura resumir a análise.

As FFAA assumem uma estrutura CSIRT distribuída, com NCIRT em cada Ramo e, futuramente, um NCIRT no EMGFA (a estrutura atual não contempla este NCIRT). Nesta estrutura distribuída, como indicado no NIST, deve haver uma entidade coordenadora de todas as outras. No caso das FFAA portuguesas, esta responsabilidade é desempenhada pelo PRTCERTDEF do COCiber (responsável pela direção técnica, monitorização e coordenação da resposta a incidentes das redes da DN).

Tal como no NIST, existem outras entidades da Organização que podem apoiar as Equipas de resposta a incidentes (do PRTCERTDEF e restantes NCIRT). Na estrutura do **COCiber** e do **gabinete do EMGFA**, as entidades são:

- Do EM a C0, a C2, a C3, a C5, a C7 e a C9.
- Das OPSCiber o BWC e o IWC.
- Das FOCiber, o Núcleo de Conhecimento Situacional e o Núcleo de Exploração da Secção de Informações Táticas, a Secção de Defesa, a Secção de Resposta e a Secção de Investigação Digital.

- Do DSCiber, a Secção de Tecnologias de Ciberdefesa e a Secção de Auditorias e Análise de Vulnerabilidades.
- O gabinete do EMGFA (no âmbito dos assuntos públicos).

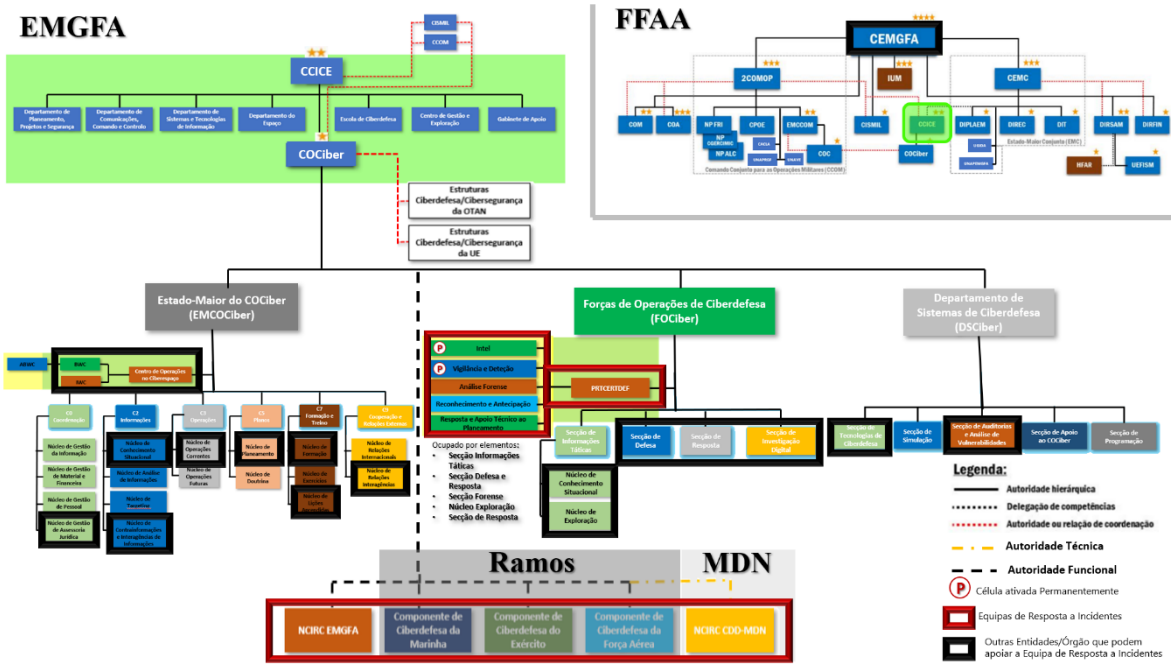


Figura 20 - Macroestrutura da CSIRC do EMGFA

Fonte: Adaptado a partir de EMGFA (2021, pp. 2-25).

No **Exército**, a estrutura CSIRT é distribuída dentro da DCSI (deixa de existir com a nova reestruturação, passando a ser a DCI a assumir as suas funções), entre o CTms (que por sua vez também descentraliza os seus meios entre os Departamentos e o ModTACTCIRC do BTms) e o NuclCIRCEx.

O NuclCIRCEx tem uma estrutura diferente do PRTCERTDEF. Pela análise das possibilidades e estrutura, deduz-se que o apoio técnico, a administração das redes, a gestão da SegInf, a análise forense e a avaliação do risco são asseguradas pelo ModTactCIRC e/ou outros órgãos da DCSI.

Tal como no NIST, existem outras entidades da DCSI que podem apoiar as Equipas de resposta a incidentes, nomeadamente a Repartição de Sistemas de Informação (RSI), Repartição de Gestão da Informação e Conhecimento, e Repartição de Guerra da Informação.

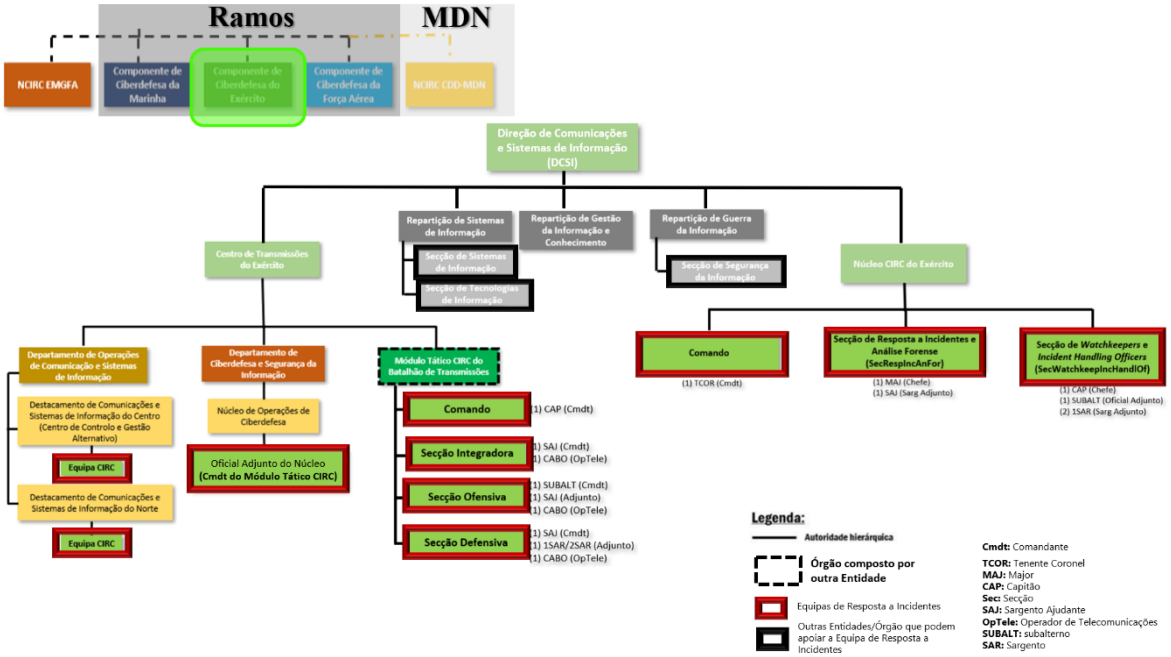


Figura 21 - Macroestrutura da CSIRT do Exército

Fonte: Adaptado a partir de EME (2016, pp. 22-23), EME (2017a, pp. 3-17) e EME (2017b, pp. 3-5).

A **Marinha** difere do PRTCERTDEF, assumindo uma estrutura CSIRT distribuída (na DITIC) como o Exército, com uma composição e articulação diferente. O GPNS integra as ETIR, para assegurar uma resposta adequada na resolução de incidentes, em 5 áreas técnicas (energia, MMHS, redes, serviços e telecomunicações). O NCIRC (chefiado em acumulação por um oficial do GPNS), em situações de resposta a incidentes é reforçado por elementos técnicos de outras Direções da DITIC. O GPNS articula-se com o NCIRC para efeitos de análise do risco e propostas de medidas de mitigação de vulnerabilidades. Ambos, encontram-se a um nível hierárquico superior às restantes Direções da DITIC.

Tal como no NIST, existem outras entidades da DITIC que apoiam NCIRC, nomeadamente a DAC/SAR, além da ETIR (que por sua vez, os seus elementos provêm da DAC e da DSE).

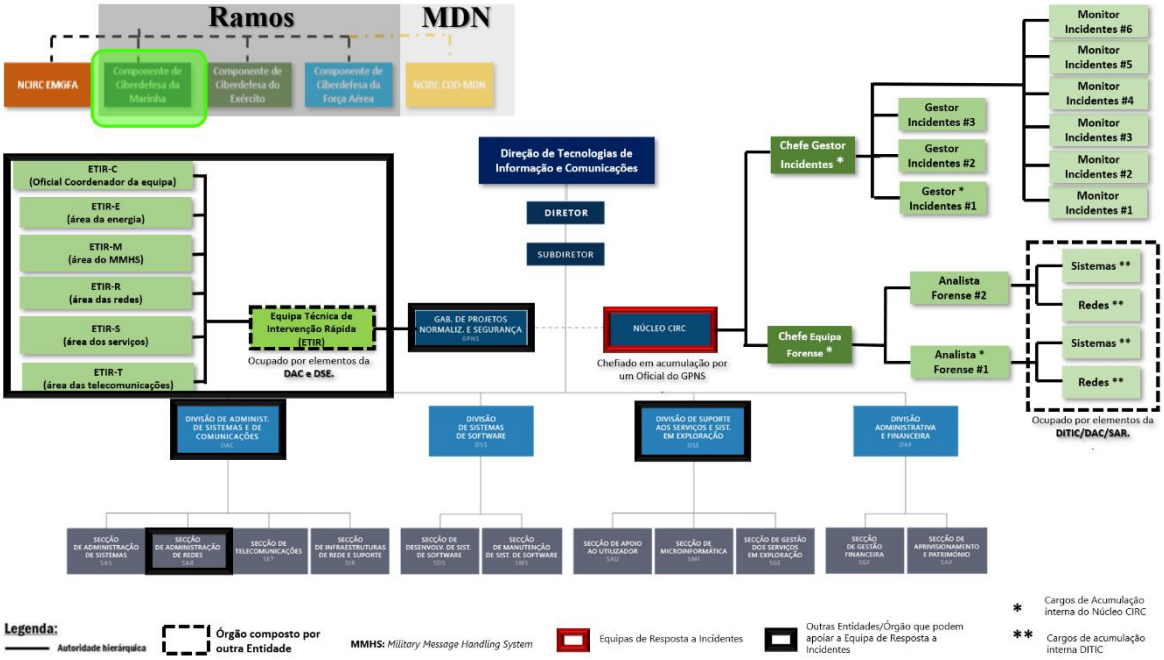


Figura 22 - Macroestrutura da CSIRC da Marinha

Fonte: Adaptado a partir de NCIRC da Marinha (Apresentação PowerPoint enviada por email, 20 de abril de 2023) e EMA (2016, pp. 4-5).

Na **FA**, apesar de não se identificar claramente o NCIRT na sua estrutura, através das funções previstas na Sub-Repartição de Segurança Informática e Ciberdefesa é possível localizá-lo na RTI da DCSI.

Tal como o PRTCERTDEF, a FA assume uma estrutura CSIRT central (difere do Exército e Marinha), integrada na Repartição de Tecnologia de Informação da DCSI do CLAFA, contudo, com uma composição e articulação diferente do Exército, Marinha e PRTCERTDEF.

Tal como no NIST, existem outras entidades da DCSI que apoiam o NCIRC, nomeadamente, da RSI e Secção de Suporte a Sistemas de Tecnologias de Informação (SSTI) no apoio técnico e administração de redes.

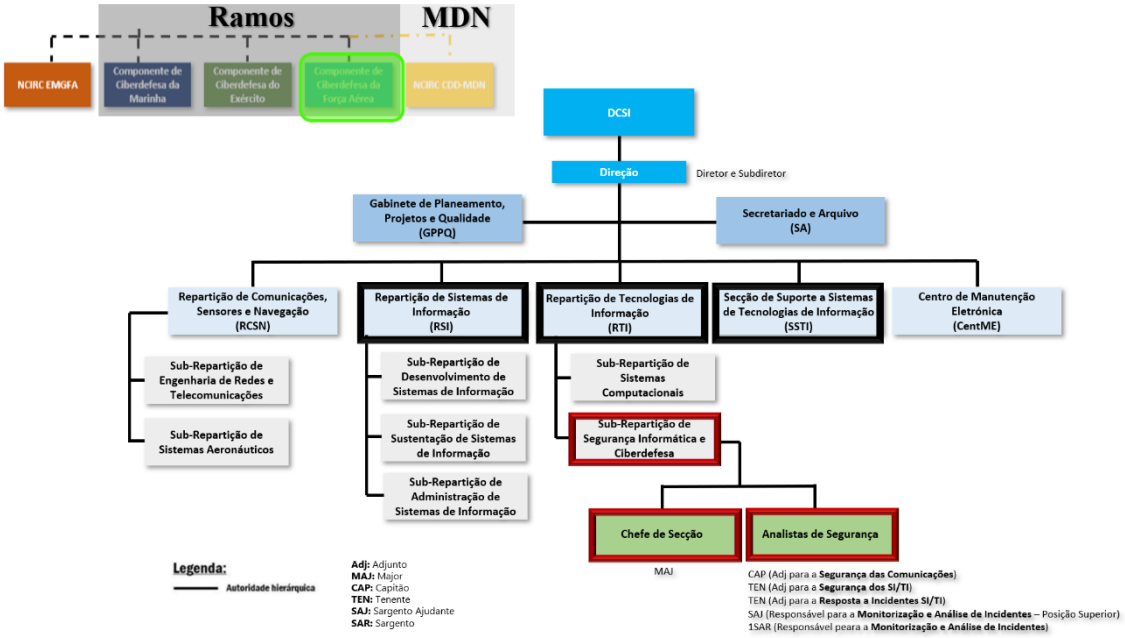


Figura 23 - Macroestrutura da CSIRT da FA

Fonte: Adaptado a partir de FA (2013, p. 8-4), FA (2022, p. A-1) e CEMFA (2019, p. 281).

De um modo geral, o PRTCERTDEF (EMGFA) e as CIRT dos Ramos incluem as entidades, funções e responsabilidades das Equipas de resposta a incidentes previstas no NIST. Contudo, identificaram-se algumas possíveis lacunas (de acordo com os indicadores em estudo) e a respetiva classificação de severidade de cada (Apêndice I), a partir do qual foi elaborado o seguinte quadro, resumo, de lacunas das FFAA.

Quadro 1 – Resumo das lacunas identificadas nas FFAA

CSIRC nas FFAA Portuguesas	Ind./ Severidade
• Não foi identificada a existência de um plano de resposta para um escalar de um incidente nas FFAA ou a definição de pontos de transição e escalonamento no processo de gestão de incidentes.	P
• Cada NCIRT dos Ramos tem uma estrutura, composição e articulação diferente entre Ramos e do PRTCERTDEF (EMGFA/COCiber).	EST
• As funções e responsabilidades entre os diversos CIRT não são idênticos, não prevendo na sua maioria a função do Líder de Incidente e Líder Técnico do incidente.	R
• Cada NCIRT dos Ramos localiza-se em patamares hierárquicos diferentes dentro do respetivo Órgão (patamar superior, equivalente ou subordinado às Direções/Repartições/Sub-repartições).	EST
• A descentralização de pessoal e meios CIRC nos Ramos, dificulta a articulação e incrementa a necessidade de controlo e coordenação.	EST
• Os Ramos têm uma estrutura mais reduzida comparativamente ao PRTCERTDEF, o que reduz a eficácia da capacidade de tratamento do incidente ao nível do Ramo.	O/E
• Elevada dependência e necessidade de apoio de outros Órgãos do Ramo ou do PRTCERDEF do COCiber, na monitorização das redes, *situational awarness*, análise forense, gestão de risco, assessoria jurídica, lições aprendidas, assuntos públicos, gestão da SegInf, apoio técnico.	O/E
• Face à dimensão e estrutura das FFAA, descentralização das CIRT, aos efeitos operacionais e estratégicos resultantes do escalar de um incidente, ao patamar de decisão e à necessidade de uma resposta ao incidente única e integrada por toda a organização, verifica-se que não existe definido um grupo de apoio à decisão para: o Gerir a crise ao nível operacional e estratégico. o Gerir as várias entidades envolvidas diretamente ou no apoio à resposta ao incidente. o Apoiar o patamar hierárquico superior no esclarecimento da situação, na avaliação dos riscos e na decisão das medidas a adotar para a mitigação dos danos e resolução do incidente. o Apoiar o patamar subordinado através do *situational awareness*, no cumprimento e gestão do plano de resposta ao incidente, no controlo e gestão da informação e da comunicação, na coordenação da ligação entre entidades internas e externas, no acompanhamento da situação, no processo de lições aprendidas e implementação de medidas de melhoramento, prevenção e correção para situações futuras.	O/E

LEGENDA:	
IND: Indicador	**O/E:** Órgão/Entidade
P: Processo	**R:** Responsabilidade
EST: Estrutura	

GRAU DE SEVERIDADE	
Catastrófico (I)	Perda de capacidade para cumprir a missão ou falhar o cumprimento da missão (...)
Crítico (II)	Degradação significativa (severa) na capacidade para cumprir a missão ou na prontidão da unidade (...)
Marginal (IV)	Degradação da capacidade de cumprimento da missão na prontidão da unidade (...)
Negligenciável (IV)	Pouco ou nenhum impacto negativo na operação (...)

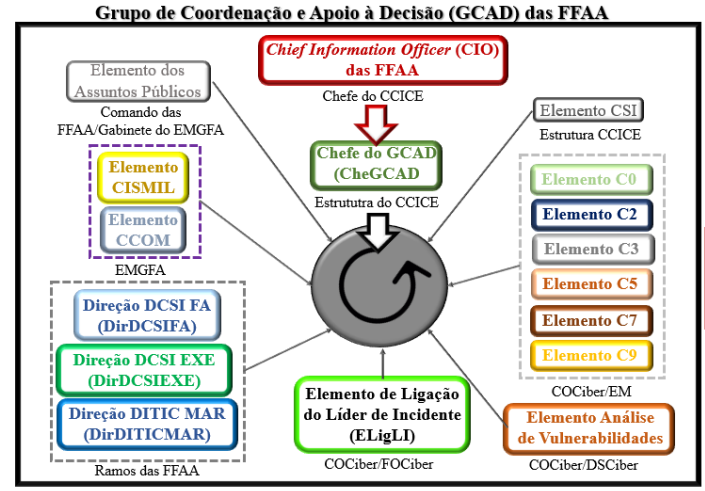
Fonte: Autor (2023).

Assim, dando **resposta à QD2**, podemos concluir que a **estrutura, processos e responsabilidades previstos no novo decreto regulamentar das FFAA, na escalada de resposta a ciberincidentes, não se encontram totalmente adequadas**.

6. Estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes

Neste último capítulo, com base nas lacunas referidas anteriormente, **responde-se à QC, que estrutura, processos e responsabilidades devem ser criados nas FFAA, na escala de resposta a ciberincidentes?**

Perante uma situação de crise, cujos efeitos podem ter impacto ao nível operacional e estratégico das FFAA e na própria soberania nacional, deve ser criado um Grupo de Coordenação e Apoio à Decisão (GCAD). Este GCAD seria composto por diversas entidades da estrutura das FFAA (cada uma assegurando um POC principal e alternativo), de modo a gerir a situação de crise, garantir a orientação, integração e gestão das várias entidades envolvidas no processo de decisão e assegurar uma resposta estratégica das FFAA, na sequência da escalada de um ciberincidente. De seguida, apresentam-se as entidades que integrariam este GCAD e as respetivas responsabilidades.



Responsabilidades do GCAD
- Gerir a crise (ciberincidente) e o processo de tomada de decisões, ao nível operacional e estratégico, com base no risco; e assegurar uma resposta estratégica das FFAA.
- Garantir a orientação, integração e gestão das várias entidades envolvidas, diretamente ou no apoio, à resposta ao incidente.
- Coordenação geral das atividades, técnicas e não técnicas, de gestão da resposta a ciberincidentes (durante o tratamento do incidente e pós-incidente).
- Apoiar o patamar hierárquico superior (estratégico) no esclarecimento da situação, na avaliação dos riscos e na decisão das medidas a adotar para a mitigação dos danos, resolução do incidente, recuperação e continuidade dos serviços.
- Apoiar o patamar subordinado através do *situational awareness;* no cumprimento e gestão do plano de resposta ao incidente; no controlo, gestão e partilha da informação e da comunicação; na coordenação da ligação entre entidades internas e externas; no seguimento do processo de escalada; no processo de lições aprendidas; e implementação de medidas de melhoramento, prevenção e correção para situações futuras.

Responsabilidades CIO das FFAA
- Tomar decisões de acordo com o risco do ciberincidente para as FFAA, enquanto autoridade técnica no âmbito das CSI, GE, e SegInf, e autoridade funcional e técnica no âmbito da ciberdefesa.
- Assegura que todas as entidades necessárias estão envolvidas no processo de gestão do incidente.
- Assegura a colaboração com os Comandos Operacionais e entidades, para a compreensão e mitigação das implicações operacionais.

Responsabilidades CheGCAD
- Convocar as entidades necessárias (ao nível operacional e estratégico), para gerir o processo de resposta ao ciberincidente.
- Liderar as atividades do GCAD.
- Analisar as implicações do incidente e avaliar os possíveis danos (Estratégico, Legal, Político…).
- Assegurar a partilha de informação relevante.
- Assegurar o cumprimento do Plano de Reação, Mitigação e Recuperação de Incidentes nas FFAA.
- Coordenar as respostas ao incidente e tomar decisões de gestão de risco.
- Assegurar a resposta adequada ao incidente, entre os Ramos e o EMGFA.
- Assegurar as atividades de Lições Aprendidas.

Responsabilidades Elemento do EM do COCiber
- C0 (Assegurar a assessoria jurídica).
- C2 (Identificação de ameaças para reduzir e mitigar o risco; analisar, processar e disseminar as informações).
- C3 (Avaliação de impacto de efeitos; coordenação dos esforços de mitigação com os responsáveis dos sistemas; e na manutenção do conhecimento situacional).
- C5 (Atualização do risco).
- C7 (Desenvolvimento do processo de lições aprendidas).
- C9 (Assegurar a coordenação e cooperação interagências, com o CNCS, o CERT Portugal, a PJ, o SIS, o CERT.PT, outros organismos nacionais e internacionais (OTAN).

Responsabilidades Elemento CSI
Aconselhar (enquanto especialista CSI) e apoiar o processo de gestão do incidente.

Responsabilidades Elemento Assuntos Públicos
Assegurar o apoio no âmbito dos assuntos públicos (media…).

Responsabilidades ELigLI
- Assegurar a ligação entre o Líder de Incidente e o GCAD.
- Apoiar o GCAD em assuntos técnicos e de segurança.

Responsabilidades Elemento Análise de Vulnerabilidades
Responsável pela gestão do risco e dos potenciais impactos nos sistemas das FFAA, e pelas propostas e avaliação das medidas de resposta ao risco associadas às vulnerabilidades encontradas.

Responsabilidades Elementos da Direção CSI/TI dos Ramos
- Representar o Ramo.
- Apoiar o GCAD na avaliação estratégica com base no risco, no esclarecimento situacional do Ramo, na gestão da resposta ao incidente e nas coordenações com o Ramo.

Responsabilidades Elementos CISMIL e CCOM
- CISMIL (No âmbito das informações no ciberespaço e segurança, apoiar o processo de gestão de incidentes; e analisar as informações recebidas do incidente, no âmbito do estudo e avaliação de ameaças).
- CCOM (Assegurar a ligação entre o CCOM e o GCAD; apoiar na avaliação do impacto do ciberincidente para as Operações e Missões das FFAA.

Figura 24 - Macroestrutura do GCAD das FFAA, selecionado

Fonte: Autor (2023).

Destas entidades, importa salientar as seguintes particularidades relativas à sua proveniência, referindo a importância do Chefe da GCAD ser um elemento não técnico, permitindo ter uma visão mais abrangente ao nível estratégico.

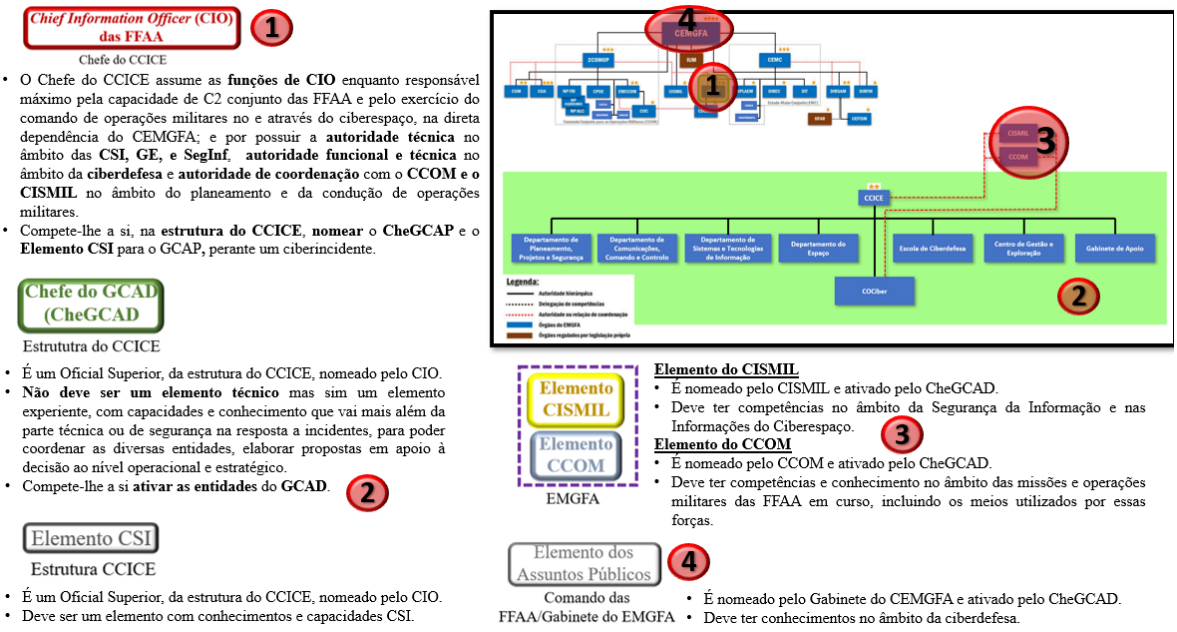


Figura 25 - Proveniência e ativação das entidades que integrariam o GCAD

Fonte: Autor (2023).

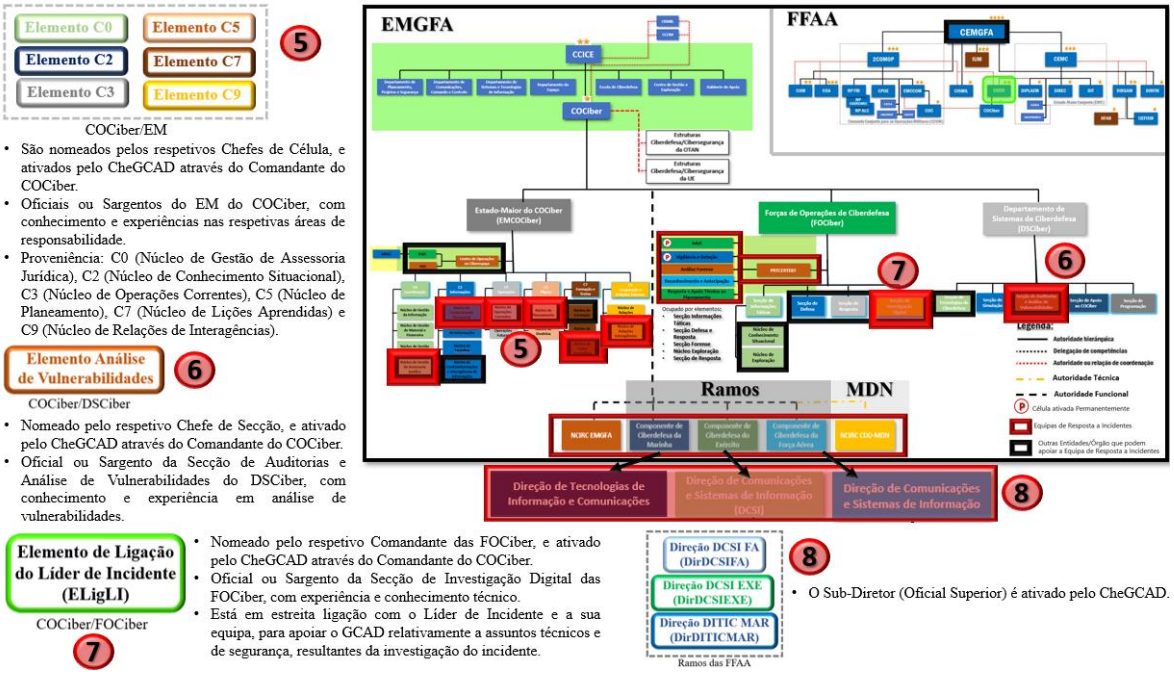


Figura 26 - Proveniência e ativação das entidades que integram o GCAD

Fonte: Autor (2023).

Em sintonia com o NIST, relativamente à estrutura CSIRC das FFAA sugere-se, além da implementação prevista do NCIRT do EMGFA, que se mantenha uma estrutura distribuída, sendo o PRTCERTDEF a CIRT coordenadora de todas as outras. Contudo, ao nível do Ramos, nomeadamente o Exército e Marinha, passe a ter uma estrutura CIRT Central.

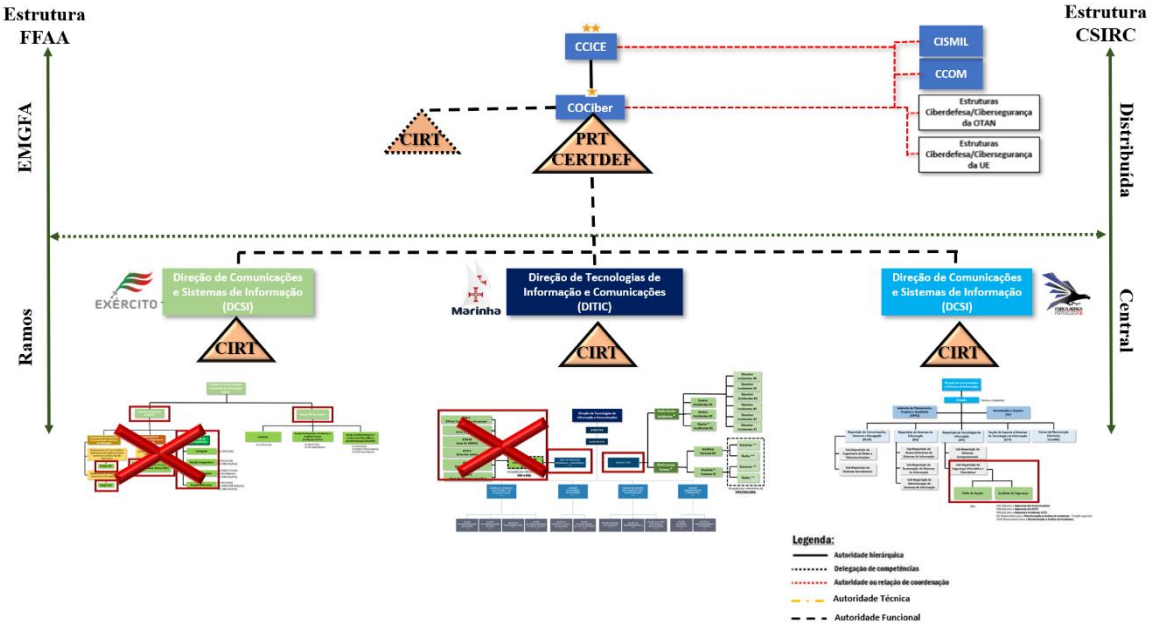


Figura 27 - Estrutura CSIRC das FFAA

Fonte: Autor (2023).

Ao nível do EMGFA/COCiber (enquanto autoridade técnica e funcional do NCIRT do EMGFA e dos Ramos), sugere-se que ao PRTCERTDEF (responsável pelo acompanhamento, deteção, análise e resposta ao nível tático) sejam acrescentadas as responsabilidades:

- Função do LI (POC principal responsável pelo tratamento do incidente e por recolher informações da equipa e comunicar para outros grupos), à semelhança do CIRT do Exército que tem os *Incident Handling Officers*; e do LT (para supervisão do trabalho técnico da equipa).
- Análise do risco, a cargo do Chefe de Divisão ao PRTCERTDEF; e uma Equipa Modular Destacável (EMD), para liderar atividades técnicas, de segurança e investigação na resposta aos incidentes, em apoio dos Ramos e do EMGFA.

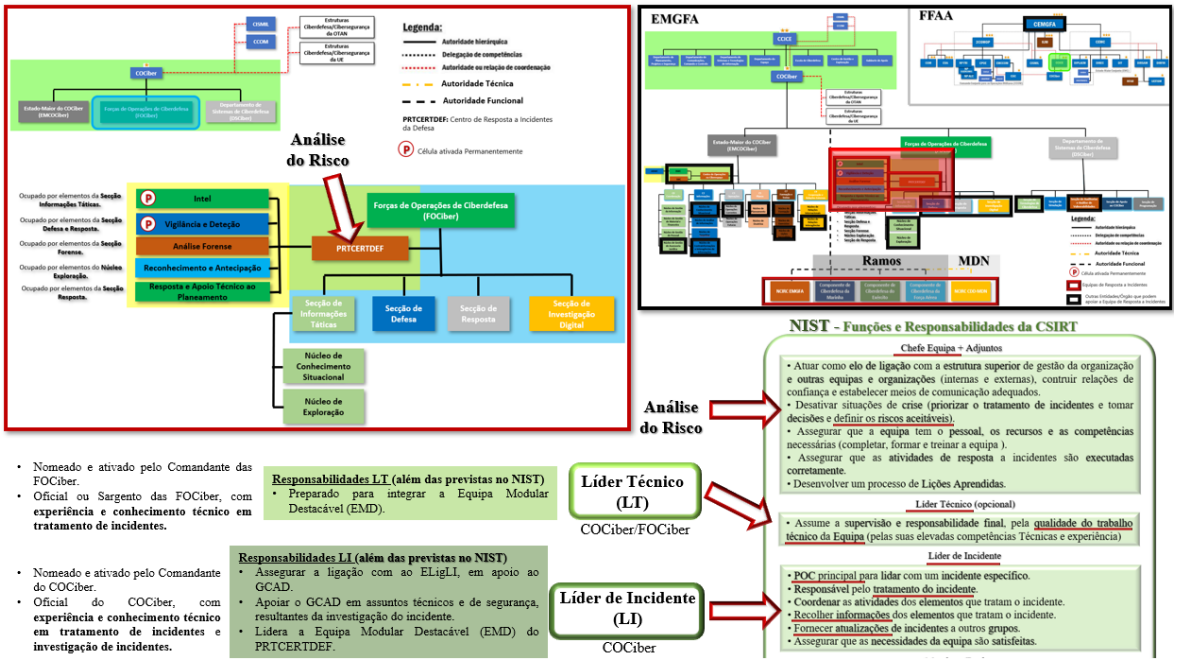


Figura 28 - Acréscimos de responsabilidades (LT, LI e Análise Risco) ao PRTCERDEF, sugeridas

Fonte: Autor (2023).

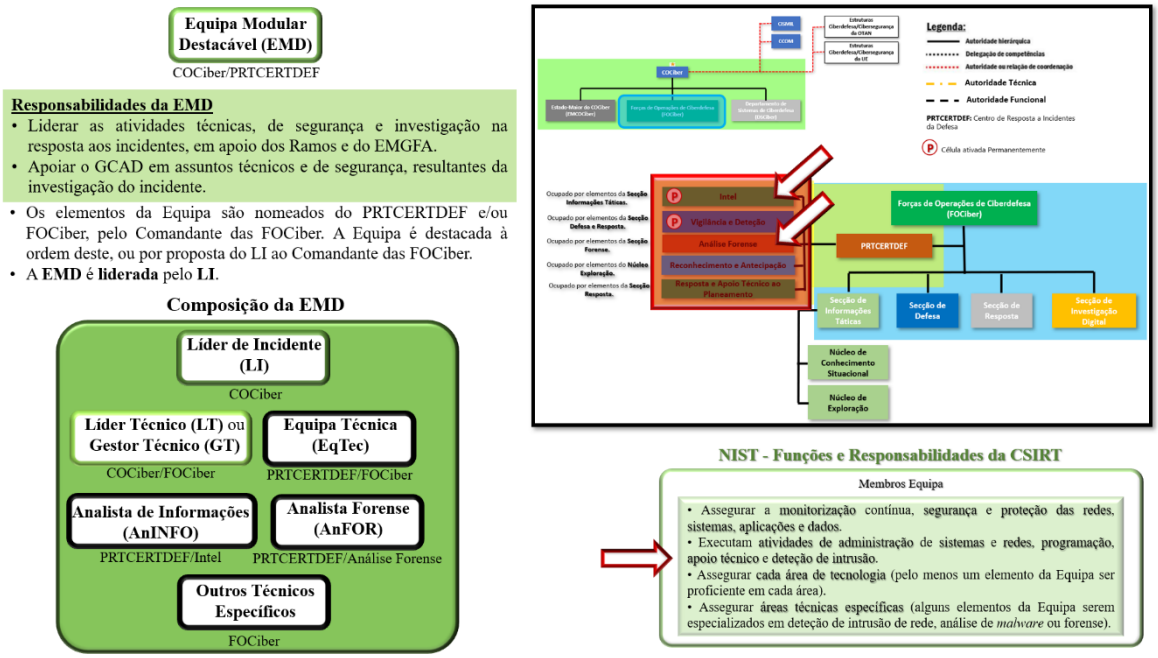


Figura 29 - Acréscimos de responsabilidades (EMD) ao PRTCERTDEF, sugerida

Fonte: Autor (2023).

Ao nível dos Ramos, sugerem-se as seguintes alterações aos NCIRT:

- Incluir as responsabilidades do LI, do LT e as restantes previstas no NIST.
- Passem a ter uma estrutura o mais similar possível ao PTRCERTDEF, com capacidades de Vigilância e Deteção (permanentes), de Análise Forense e de Resposta e Apoio Técnico ao Planeamento, para conferir uma maior capacidade e autonomia ao Ramo no tratamento de incidentes (reduzir a dependência do COCiber), mesmo que seja com uma composição menor (efetivos), comparativamente ao PRTCERTDEF.
- Que a sua estrutura e articulação seja idêntica nos três Ramos, melhorando o controlo e coordenação.
- Que estejam localizados (estruturalmente) na respetiva Direção do Ramo, o mais próximo possível do poder de decisão (entre a Chefia das Direções e as Repartições). Exceção, para quando for criada a capacidade de ciberdefesa nos Ramos, neste caso, integrando na estrutura desta capacidade.

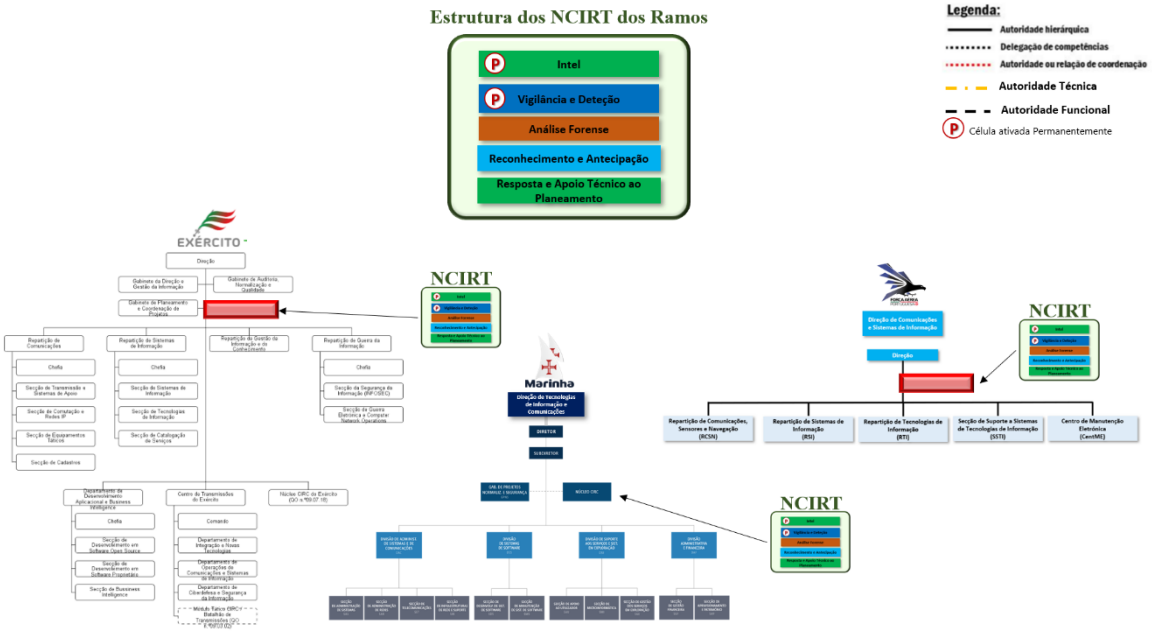


Figura 30 - Estrutura dos NCIRT dos Ramos, sugerida

Fonte: Autor (2023).

Por último, em termos dos processos, é essencial que estas novas entidades/responsabilidades/estrutura sugeridas estejam vertidas num Plano de Reação, Mitigação e Recuperação de Incidentes das FFAA. Este plano deve:

- Ter em conta as fases de Preparação; Deteção e Análise; Contenção, Erradicação e Recuperação; e Atividade Após o Incidente (de acordo com o NIST).
- Considerar que pode ocorrer mais do que um incidente e que, paralelamente, continuam a decorrer as operações no ciberespaço, por parte da capacidade de ciberdefesa das FFAA.
- O GCAD deve ser sempre ativado perante um ciberincidente, mesmo que a avaliação inicial não indique um provável escalar para as FFAA. Isto irá permitir iniciar os processos e avaliações necessárias, conferindo antecipação em caso de alteração da situação ou de novos incidentes consequentes.
- Estabelecer um processo de escalada de ciberincidentes e definir os pontos de transição, para os casos em que a gravidade do incidente o exija ou se a equipa não responder a um incidente dentro do tempo estipulado (definindo o tempo de espera por uma resposta; o que fazer se não houver resposta, indicando quem reage e como se reage). Para tal, cada entidade ao seu nível (Ramos e EMGFA) deve ter em consideração a avaliação do impacto do incidente. Esta avaliação pode ser feita com base no impacto funcional (o impacto negativo atual e futuro nas funções da organização), o impacto informativo (o efeito relativo à confidencialidade, integridade e disponibilidade das informações da organização) e a recuperabilidade do incidente (o tempo e tipos de recursos que devem ser gastos na recuperação do incidente). Deste modo, mais facilmente será possível avaliar os riscos e definir as prioridades.

6.1 Cenarização

De seguida, procura-se traduzir algumas das considerações, referidas anteriormente, para o plano através de três cenários, tendo em comum a fase da ativação das entidades envolvidas na resposta a ciberincidentes:

- **Ativação** do GCAD, perante a deteção de um ciberincidente.

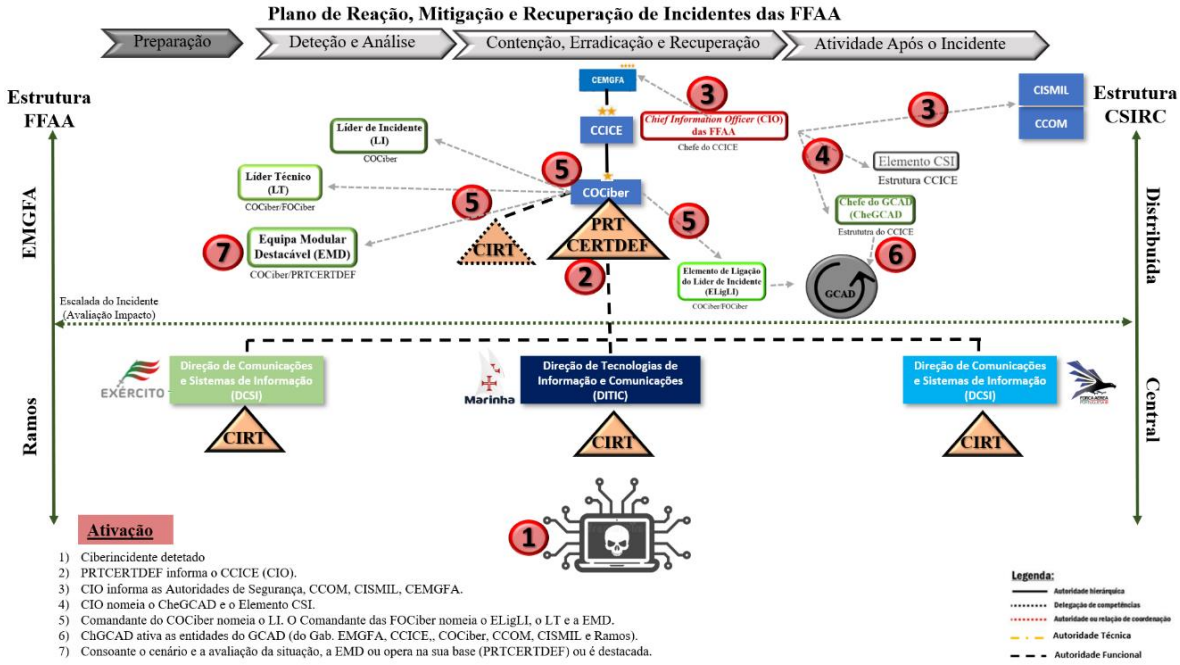


Figura 31 – Considerações para o plano de reação (ativação)

Fonte: Autor (2023).

- **Cenário 1**, em que um incidente ocorre num Ramo das FFAA e avalia-se que o Ramo tem capacidade para resolver ou é improvável um escalar do incidente.

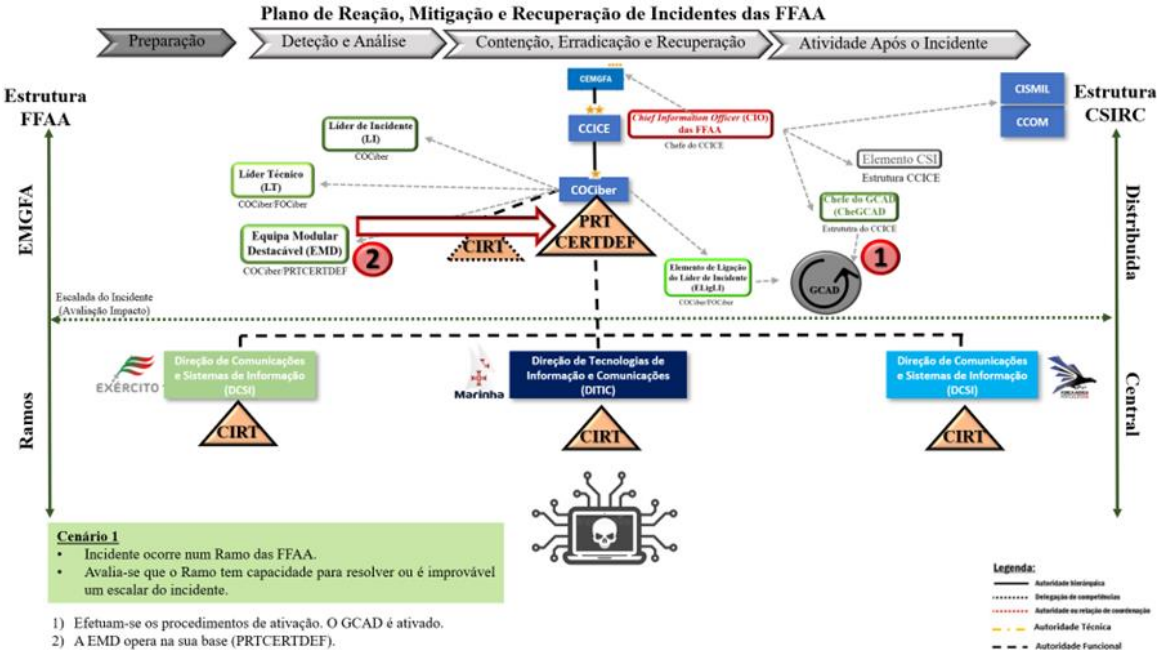


Figura 32 - Considerações para o plano de reação (cenário 1)

Fonte: Autor (2023).

- **Cenário 2**, em que um incidente ocorre ao nível da estrutura do EMGFA.

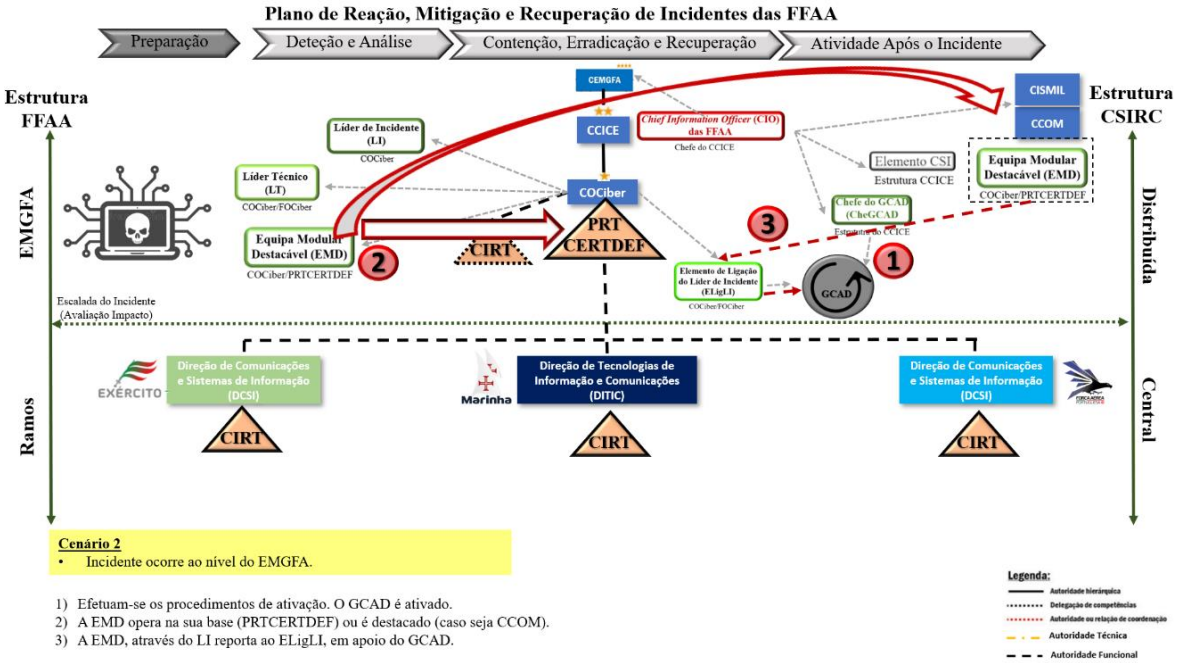


Figura 33 - Considerações para o plano de reação (cenário 2)

Fonte: Autor (2023).

- **Cenário 3**, em que um incidente ocorre num ou mais Ramos das FFAA e avalia-se que o Ramo não tem capacidade para resolver ou é provável o escalar do incidente.

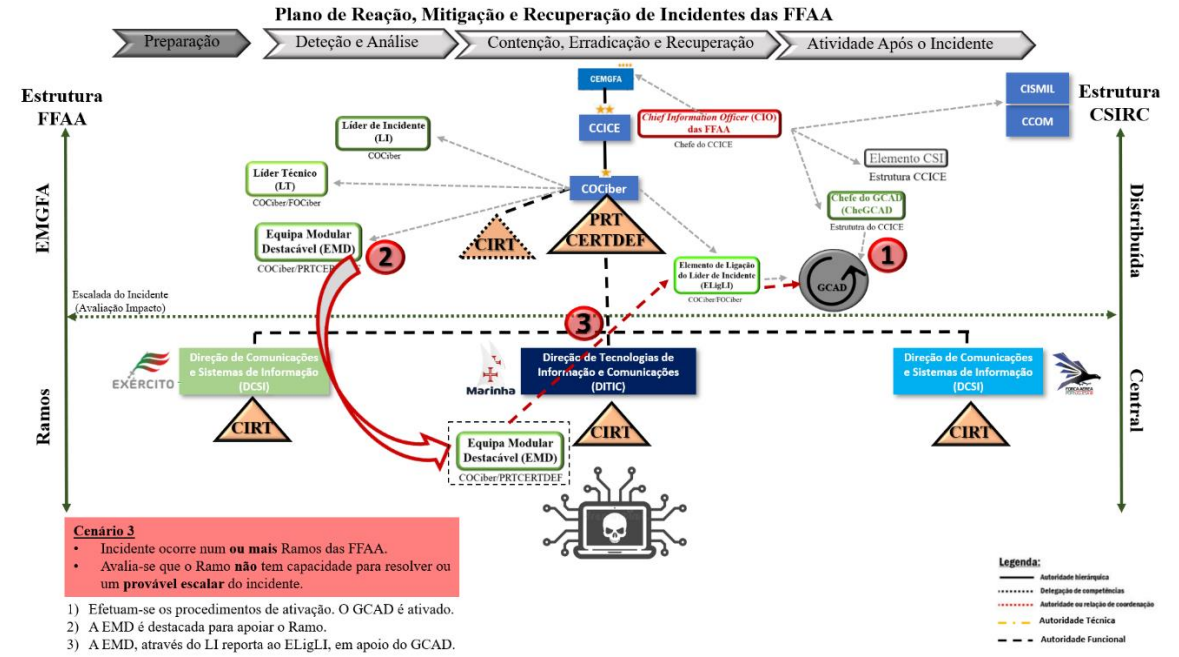


Figura 34 - Considerações para o plano de reação (cenário 3)

Fonte: Autor (2023).

7. Conclusões

O Ciberespaço é um domínio transversal a todos os outros, explorado por novas formas de ameaça, onde os ataques são cada vez mais frequentes, diversificados e com efeitos mais disruptivos. Os riscos aumentam com o incremento da dependência das sociedades na tecnologia e infraestruturas tecnológicas, e com as falhas de segurança por parte das organizações, uma vez que, a informação capturada pode ameaçar a segurança nacional ou a sobrevivência das principais instituições do Estado.

É essencial a edificação de capacidades de ciberdefesa e cibersegurança nas FFAA, exigindo a estas a preparação e capacitação para uma adequada gestão de incidentes, através de um processo que permita uma resposta pronta, clara e eficiente, para assegurar a proteção das pessoas, dados e processos.

A nova LOEMGFA veio conferir ao COCiber, a autoridade técnica e funcional sobre os Ramos na capacidade de ciberdefesa, passando a existir uma maior influência e coordenação entre o CSIRC do EMGFA e o CSIRC dos Ramos.

De modo a verificar, se as FFAA estarão preparadas para responder a ciberincidentes, este estudo teve como objetivo, **selecionar a estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes**,

Através da análise documental, a partir da *framework* de boas práticas de resposta a incidentes do NIST procurou-se identificar a estrutura, processos e responsabilidades existentes numa escalada de resposta a Ciberincidentes, para posteriormente comparar-se à nova organização das FFAA (prevista na nova LOEMGFA), identificando-se possíveis lacunas nas CSIRC do EMGFA e dos Ramos (tendo como indicadores os processos, responsabilidades, órgãos, funções, entidades e grupos de tomada de decisão envolvidos na resolução de incidentes). Com base nessas lacunas, selecionou-se dedutivamente o processo, estrutura e as responsabilidades a serem criados, na escalada de resposta a Ciberincidentes das FFAA portuguesas.

Do estudo verificou-se que a CSIRC das FFAA portuguesas deve manter-se uma estrutura distribuída, implementando o previsto Núcleo CIRC do EMGFA. Contudo, ao nível dos Ramos, estes devem passar a ter uma CIRT central, mantendo-se a PRTCERTDEF como a CIRT coordenadora de todas as outras. A esta, devem ser acrescentadas: as responsabilidades inerentes às funções do LI (POC principal responsável pelo tratamento do incidente e por recolher informações da equipa e comunicar para outros grupos) e do LT (para supervisão do trabalho técnico da equipa); a análise do risco (a cargo do Chefe de

Divisão ao PRTCERTDEF); e uma EMD (para liderar atividades técnicas, de segurança e investigação na resposta aos incidentes, em apoio dos Ramos e do EMGFA). Para os CSIRC dos Ramos, sugerem-se que: a estrutura e articulação seja idêntica nos três Ramos (para melhorar o controlo e coordenação); localizada o mais próximo possível do poder de decisão (entre a Chefia das Direções e as Repartições); inclua as responsabilidades do LI, do LT e as restantes previstas no NIST; passe a ter uma estrutura o mais similar possível ao PTRCERTDEF (com capacidade de Vigilância e Deteção permanentes; Análise Forense e de Resposta e Apoio Técnico ao Planeamento) para conferir uma maior capacidade e autonomia ao Ramo, no tratamento de incidentes.

Deve ser criado um GCAD, de modo a gerir a situação de crise, garantir a orientação, integração e gestão das várias entidades envolvidas no processo de decisão e assegurar uma resposta estratégica das FFAA, na sequência da escalada de um ciberincidente. Este grupo seria composto composto por diversas entidades: O Chefe do CICCE (enquanto CIO das FFAA); o CheGCAD (responsável por convocar e liderar as atividades do GCAD); o ELigLI (para apoiar o GCAD em assuntos técnicos e de segurança); o Elemento CSI (para aconselhar e apoiar o processo enquanto especialista); o Elemento dos Assuntos Públicos (para apoiar no enquanto especialista); o Elemento do CISMIL (para apoiar no âmbito do estudo e avaliação de ameaças); o Elemento do CCOM (para apoiar na avaliação do impacto do ciberincidente para as Operações e Missões das FFAA); o Elemento de Análise de Vulnerabilidades (responsável pela gestão do risco e dos potenciais impactos nos sistemas das FFAA, pelas propostas e avaliação das medidas de resposta ao risco); e os elementos do EM do COCiber, da C0 (assegurar a assessoria jurídica), da C2 (identificação de ameaças para reduzir e mitigar o risco; analisar, processar e disseminar as informações), da C3 (avaliação de impacto de efeitos; coordenação dos esforços de mitigação com os responsáveis dos sistemas; e manutenção do conhecimento situacional), da C5 (atualização do risco), da C7 (desenvolvimento do processo de LA), da C9 (assegurar a coordenação e cooperação interagências com o CNCS, o CERT Portugal, a PJ, o SIS, o CERT.PT, outros organismos nacionais e internacionais).

Em termos dos processos, deve ainda ser criado um Plano de Reação, Mitigação e Recuperação de Incidentes das FFAA (contemplando as fases de Preparação; Deteção e Análise; Contenção, Erradicação e Recuperação; e Atividade Após o Incidente), considerando a ocorrência de mais do que um incidente em simultâneo e a continuação das operações no ciberespaço por parte da capacidade de ciberdefesa das FFAA; a ativação do

GCAD, mesmo que a avaliação inicial não indique um provável escalar para as FFAA (para permitir iniciar os processos e avaliações necessárias, em antecipação a uma alteração da situação ou de novos incidentes consequentes) e os cenários de emprego (o incidente ocorre num dos Ramos, sendo improvável um escalar do incidente; o incidente ocorre ao nível do EMGFA; e o incidente ocorre num ou mais Ramos, sendo provável o escalar do incidente); e a definição dos pontos de transição do processo de escalada de ciberincidentes, de acordo com a gravidade e impacto do incidente ou se a equipa não responder dentro do tempo estipulado (referindo o tempo de espera por uma resposta; o que fazer se não houver resposta, indicando quem reage e como se reage).

Este estudo contribui para as FFAA, nomeadamente, para o COCiber e para as componentes de ciberdefesa dos Ramos, através da identificação de lacunas e respetiva sugestão de melhorias para a capacidade de resposta a ciberincidentes.

As principais limitações no desenvolvimento do trabalho, deveram-se ao fato de ainda não ter sido aprovada a nova restruturação dos Ramos, o que exigiu a análise da última documentação em vigor (não prevendo ainda as alterações da nova LOEMGFA), por sua vez, em alguns casos dos Ramos, esta encontra-se desatualizada e por vezes pouco pormenorizada (sobre a composição e responsabilidades das CIRT); por outro lado, a existência de pouca informação relativa à constituição do NCIRT do EMGFA e a diferença cultural, de cada Ramos e do EMGFA, na forma de documentar a informação (uns utilizam os Quadros Orgânicos, outros utilizam Regulamentos Internos ou apresentações PowerPoint), o que dificultou a análise comparativa entre as CIRT; e por último, não foram executadas entrevistas de validação (por motivos de tempo) relativamente às propostas apresentadas.

Como estudos futuros, sugere-se complementar este estudo com a nova restruturação dos Ramos ao nível da sua capacidade de ciberdefesa (assim que estas forem aprovadas), bem como, estender o âmbito do atual estudo por forma a incluir os Núcleos CIRC do MDN e do EMGFA (assim que este for implementado e que exista documentação sobre o mesmo).

Referências bibliográficas

Centro Nacional de Cibersegurança [CNCS]. (2019a). *Estratégia Nacional de Segurança do Ciberespaço.* Lisboa: CNCS.

Centro Nacional de Cibersegurança. (2019b). *Quadro Nacional de Referência para a Cibersegurança.* Lisboa: CNCS.

Chefe de Estado Maior da Força Aérea [CEMFA]. (2019). *Parte 27 – Estrutura Orgânica - Direção de Comunicações e Sistemas de Informação – DCSI – (Código: 1E200).* Lisboa: CEMFA.

Comando da Logística da Força Aérea [CLFA]. (2013). *MCLAFA 305-2 - Organização e Normas de Funcionamento da Direção de Comunicações e Sistemas De Informação*, de outubro. Lisboa: CLFA.

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, Série I de 2022-01-24. Lisboa: Presidência do Conselho de Ministros.

Estado Maior da Armada [EMA]. (2016). *Regulamento Interno da Direção de Tecnologias de Informação e Comunicações*. Lisboa: EMA.

Estado-Maior do Exército [EME]. (2016). *Quadro Orgânico 09.03.02, Batalhão de Transmissões (DCSI)*, de 15 fevereiro. Lisboa: EME.

Estado-Maior do Exército. (2017a). *Quadro Orgânico 01.02.02, Direção de Comunicações e Sistemas de Informação (DCSI)*, de 07 abril. Lisboa: EME.

Estado-Maior do Exército. (2017b). *Quadro Orgânico 09.07.18, Núcleo CIRC do Exército (NuclCIRCEx)*, de 07 abril. Lisboa: EME.

EMGFA. (2021). *Regulamento Interno do Comando de Operações de Ciberdefesa* (V1.5). Lisboa: EMGFA.

Força Aérea [FA]. (2011). *RFA 390-6 Política de Ciberdefesa da Força Aérea*, de fevereiro. Lisboa: FA.

Força Aérea. (2013). *RFA 303-4(A) Organização e Normas de Funcionamento do Comando da Logística da Força Aérea*, de outubro. Lisboa: FA.

Lei n.º 46/2018, de 13 de agosto. (2018). *Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*.

Diário da República, 1.ª Série, N.º 155, 4031 a 4037. Lisboa: Assembleia da República.

Lei Orgânica n.º 2/2021, de 09 de agosto. (2021). *Aprova a Lei Orgânica de Bases da Organização das Forças Armadas.* Lisboa: Diário da República n.º 153/2021, Série I de 2021-08-09. Lisboa: Assembleia da República.

Lei Orgânica n.º 3/2021, de 09 de agosto. (2021). *Altera a Lei de Defesa Nacional, aprovada pela Lei Orgânica n.º 1-B/2009, de 7 de julho.* Lisboa: Diário da República n.º 153/2021, Série I de 2021-08-09. Lisboa: Assembleia da República.

Lopes, F. M. S. C. (2010). *Gestão do Conhecimento – Modelação dos Incidentes e das Respostas* (Tese de Dissertação para obtenção de Grau Mestre em Segurança dos Sistemas de Informação). Universidade Católica Portuguesa, Lisboa.

Matos, D. (2018). *Gestão de Incidentes de Cibersegurança em Organizações Públicas* (Tese de Dissertação para obtenção de Grau Mestre em Engenharia Informática e de Computadores). Instituto Superior Técnico, Lisboa.

North Atlantic Treaty Organization [NATO] and the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes [NATO PfPC] (2016). *Cybersecurity a Generic Reference Curriculum*. Gernackerstrasse 2: NATO.

NATO. (2018). *High Level Taxonomy of Cyberspace Operations (Taxonomia IMSM-0222-2018)*. Bruxelas: NATO Internanacional Military Staff.

NATO. (2022, 23 de março). Cyber defence. *NATO* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm

NEP/INV - 001 (A1). (2020). *Procedimentos relativos à elaboração de Trabalhos de investigação realizados no âmbito de cursos que não atribuem Grau Académico*. Lisboa: Instituto Universitários Militar [IUM].

NEP/INV - 003 (A1). (2020). *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: IUM.

Neves, P. J. B., & Correia, F. J. R. (2016). Resposta a Incidentes de Segurança da Informação: Uma abordagem DOTMLPI-I. *Cyberlaw by CIJIC*, nº 1, pp. 1-24. Retirado de https://comum.rcaap.pt/bitstream/10400.26/18023/1/Paulo%20Batista%20das%20Neves%2016_Resposta%20a%20Incidentes%20de%20Seguran%c3%a7a%20da%20Informa%c3%a7%c3%a3o%20uma%20abordagem%20DOTMLPI-I.pdf

National Institute of Standards and Technology [NIST] (2012). *Computer Security Incident Handling Guide* (Revision 2). Gaithersburg: NIST.

Santos, L.A.B., & Lima, J. M. M. (Coord.). (2019). *Orientações Metodológicas para a elaboração de Trabalhos de Investigação.* Pedrouços: IUM.

Santos, L. C., Nunes, P. V., Ralo, J., & Mendes, C. P. (abril de 2018). Contributos Para uma Estratégia Nacional de Ciberdefesa. *Defesa do Ciberespaço*, pp. 33-46.

Apêndice A – Glossário de conceitos complementares

Ciberespaço

De acordo com o CNCS (2019a, p. 7), o Ciberespaço "Consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.". Inclui-se o:

> […] domínio virtual, de natureza global e comum, dentro do ambiente da informação, composto pelos sistemas de comunicação, informação e outros sistemas de natureza eletrónica, incluindo a sua interação e a informação, de natureza digital, que é armazenada, processada e transmitida através desses sistemas. (NATO, 2018).

Cibersegurança

A Cibersegurança é 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, disponibilidade[3] e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. (CNCS, 2019a, p. 7)

Ciberdefesa

A Ciberdefesa "consiste na atividade que visa assegurar a DN no, ou através do, ciberespaço" (CNCS, 2019a, p. 7). Trata-se do conjunto de atividades e meios "através dos quais se atingem e executam medidas defensivas para fazer face a ciberataques e mitigar os seus efeitos, preservando e restaurando assim a segurança do ciberespaço e permitindo assegurar a garantia da missão" (NATO, 2018).

Cibercrime

Cibercrime, são "os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa" (CNCS, 2019a, p. 7).

Ciberataque

É uma tentativa de obter acesso não autorizado a serviços, recursos ou informações do sistema ou uma tentativa de comprometer a integridade do sistema[4] (NATO and the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes [NATO PfPC], 2016, p. 62).

Evento e Incidente

De acordo com o NIST (2012, p. 6), um evento é qualquer ocorrência observável num sistema ou rede[5]. Eventos adversos, são eventos com uma consequência negativa[6].

Um incidente consiste em "Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação." (Lei n.º 46/2018, 2018, p. 4031).

Tratamento de incidentes / Resposta a incidentes

De acordo com a Lei n.º 46/2018, de 13 de agosto (2018, p. 4032) o tratamento de incidentes são "todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente".

O NIST (2012, p. 60) considera a mesma definição para a resposta e tratamento de incidentes, a mitigação das violações das políticas de segurança e das práticas recomendadas.

Processo e Procedimento

Um processo é o "Conjunto de atividades interrelacionadas ou interatuantes que transformam entradas em saídas.". Um procedimento é o "Modo especificado de realizar uma atividade ou um processo" (CNCS, 2019b, p. 18).

---

[3] Entenda-se confidencialidade como "A propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não autorizados.", integridade como o "A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos." e disponibilidade como a "Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada." (CNCS, 2019b, pp. 17-18).

[4] Tradução do autor de "*An attempt to gain unauthorized access to system services, resources or information or an attempt to compromise system integrity*.".

[5] Tradução do autor de "*An event is any observable occurrence in a system or network.*".

[6] Tradução do autor de "*Adverse events are events with a negative consequence…*".

Apêndice B – Fases do processo de resposta a ciberincidentes

A fase da **preparação**, além de incluir a edificação da capacidade de resposta a incidentes da organização (através da constituição e treino da equipa de resposta, aquisição das ferramentas e recursos para esta operar), engloba a prevenção de incidentes através da seleção e implementação de controlos, estabelecidos com base nos resultados das avaliações de risco, para assegurar a segurança dos sistemas, redes e aplicações. Apesar destes controlos, irá sempre persistir um risco residual. A equipa de resposta a incidentes, não sendo responsável pela prevenção de incidentes, é fundamental para o sucesso de programas de resposta a incidentes (NIST, 2012, p. 21).

A fase da **deteção e análise**, consiste em alertar a organização para a ocorrência de um incidente. Estas, são tarefas extremamente difíceis fruto dos sistemas de deteção de intrusão poderem produzir falsos casos positivos, derivados de indicadores incorretos (facilmente ocorre pela quantidade elevada, diária, de indicadores e pela necessidade de avaliação da legitimidade de cada indicador). Encontrar os incidentes de segurança ocorridos, com base em todos os indicadores, é um desafio. Perante isto, é razoável suspeitar-se que um incidente possa estar a ocorrer, decidindo e agindo em conformidade. Determinar, se um evento é na realidade um incidente, é uma questão de julgamento, pelo que, a colaboração com outros elementos técnicos e de segurança da informação, pode ser necessária para a tomada de decisão. A equipa de resposta ao incidente deve analisar e validar cada incidente, seguindo um processo pré-definido. Perante a crença da ocorrência de um incidente a equipa deve realizar, rapidamente, uma análise inicial para determinar o alcance do incidente. Todos os factos devem ser documentados pela equipa; devem ser mantidos registos sobre o estado dos incidentes (juntamente com outra informação pertinente); salvaguardar os dados do incidente e restringir o acesso aos mesmos, de acordo com a informação sensível que possam conter (NIST, 2012, pp. 21-31).

Priorizar o tratamento do incidente é talvez o ponto de decisão mais crítico no processo de tratamento do incidente. O tratamento do incidente deve ser priorizado com base nos seguintes fatores (NIST, 2012, p. 32):

- Impacto funcional do incidente, considerando como é que o incidente, atualmente e no futuro, vai ter impacto na funcionalidade dos sistemas afetados.
- Impacto do incidente na informação, tendo presente que os incidentes podem afetar a confidencialidade, integridade e disponibilidade das informações. Deve-se ter em consideração, de que forma a exfiltração de informação vai ter impacto na missão geral da organização, bem como, se a informação exfiltrada for sensível, como poderá afetar outras organizações.
- Recuperabilidade do Incidente, com base na dimensão do incidente e o tipo de recursos afetados, determinar a quantidade de tempo e de recursos que devem ser despendidos na recuperação do incidente.

A combinação do impacto funcional nos sistemas da organização e o impacto na informação da organização, permite determinar o impacto do incidente na empresa. A recuperabilidade do incidente, determina as possíveis respostas que a equipa pode adotar no tratamento do incidente. A consciência situacional, vai permitir quantificar o efeito dos próprios incidentes (NIST, 2012, p. 32).

As organizações devem estabelecer um processo de escalada, para os casos em que a gravidade do incidente o exija ou se a equipa não responder a um incidente dentro do tempo estipulado. Este processo, deve indicar o tempo de espera por uma resposta e o que fazer se não houver resposta. Quando um incidente é analisado e priorizado, a equipa de resposta tem de notificar os indivíduos apropriados, para que todos os que têm de ser envolvidos no processo possam desempenhar as suas funções. As políticas de resposta a incidentes devem incluir previsões relativas à comunicação de incidentes (no mínimo, o que deve ser comunicado, a quem e quando). A equipa deve planear e preparar vários métodos de comunicação porque, durante o tratamento de incidentes, pode ter de efetuar atualizações de situação a certas entidades, ou mesmo a toda a organização (NIST, 2012, pp. 33-34).

De acordo com a gravidade da violação de segurança detetada, a organização pode mitigar o impacto do incidente através da **contenção, erradicação e recuperação** do mesmo. É frequente durante esta fase, o ciclo do processo regressar à fase anterior para deteção e análise de ameaças ainda persistentes ou novas, e verificação da eficácia das medidas de mitigação (NIST, 2012, p. 21).

A contenção é importante que seja executada, antes que um incidente exponencie os danos ou ultrapasse os recursos necessários para o mitigar, proporcionando tempo para o desenvolvimento de uma estratégia de resolução adequada. Requer a tomada de decisões, que serão mais fáceis se existirem estratégias e procedimentos, pré-determinados, para conter o incidente. Mesmo assim, as organizações devem definir riscos aceitáveis, uma vez que, as estratégias de contenção variam em função do tipo de incidente (NIST, 2012, p. 35).

Embora o principal motivo para a recolha de provas, durante um incidente, seja a resolução do incidente, pode também ser necessário para procedimentos legais. Assim, devem ser recolhidas de acordo com os procedimentos que cumprem as leis e os regulamentos aplicáveis, desenvolvidos com o pessoal jurídico e as forças de segurança, para que qualquer prova possa ser admissível em tribunal (NIST, 2012, p. 36).

Após um incidente ter sido contido, a erradicação pode ser necessária para eliminar componentes do incidente, bem como, para identificar e mitigar todas as vulnerabilidades exploradas. Durante a erradicação, é importante identificar todos os elementos afetados dentro da organização, para que possam ser restabelecidos. Na recuperação, os administradores restabelecem os sistemas ao funcionamento normal e corrigem as vulnerabilidades, para evitar incidentes semelhantes. A erradicação e a recuperação devem ser feitas numa abordagem faseada, de modo que, as medidas de reparação sejam priorizadas (NIST, 2012, p. 37).

Atividade pós incidente e o adequado tratamento do mesmo, a organização emite um relatório (com a causa e o custo do incidente) e as medidas que devem ser adotadas para prevenir incidentes futuros (NIST, 2012, p. 21). Uma das partes mais importantes é a aprendizagem e o melhoramento, com base nas respostas aos incidentes adotadas. Estas situações devem ser aproveitadas para evoluir na reflexão de novas ameaças, melhoramento da tecnologia e de LA. A realização de reuniões de LA com todas as partes envolvidas, após um incidente grave e periodicamente, é fundamental para a melhoria das medidas de segurança e para o processo de resposta através da revisão do ocorrido (o que foi feito e a eficácia da intervenção) (NIST, 2012, pp. 21 e 38).

A longo prazo, os dados recolhidos dos incidentes são úteis para vários fins. Particularmente, o total de horas de envolvimento e o custo pode ser utilizado para justificar o financiamento adicional na equipa de resposta ao incidente. O estudo das características do incidente, pode indicar ameaças e fraquezas do sistema de segurança, bem como, mudanças nas tendências de incidentes. Estes dados podem ser reintroduzidos no processo de avaliação de risco, levando à seleção e implementação de controlos adicionais; permitem medir o sucesso da equipa de resposta e, determinar, se uma mudança nas capacidades de resposta a incidentes provoca alguma alteração no desempenho da equipa; e por último, permite a comunicação de informações sobre os incidentes com o CSIRT de nível superior, outas organizações ou entidades (NIST, 2012, pp. 39 e 47).

Apêndice C – Modelo de análise

Quadro 2 - Modelo de análise

Título	Escalada de Ciberincidentes nas Forças Armadas: Entidades e Funções						
Domínio da Investigação	Domínio	Ciências Militares					
	Área	Área de Ensino das Técnicas e Tecnologias Militares					
	Subárea	Cibersegurança					
Objeto da Investigação	A estrutura, processos e responsabilidades, do EMGFA e dos Ramos, a serem criados na escalada de resposta a ciberincidentes, face à nova organização das FFAA, prevista em 2022.						
Delimitação	Domínios	Espaço	Portugal				
		Conteúdo	À estrutura, processos e responsabilidades do EMGFA e dos Ramos, com base na nova LOEMGFA.				
		Tempo	De 24 de janeiro de 2022 (data da nova LOEMGFA) a junho de 2023 (mês durante o qual será executada a exposição oral deste trabalho de investigação).				
Problema da Investigação Problema de Investigação	Objetivo Geral (OG)		Selecionar a estrutura, processos e responsabilidades a serem criados nas FFAA, na escalada de resposta a ciberincidentes.				
	Questão Central (QC)		Que estrutura, processos e responsabilidades devem ser criados nas FFAA, na escalada de resposta a ciberincidentes?				
	Objetivos Específicos		**Questões Derivadas**	**Conceitos**	**Dimensões**	**Indicadores**	**Técnicas de recolha de dados**
	OE1: Identificar a estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes.		**QD1:** Qual a estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes?	• Ciberincidentes • Equipa de Resposta • Escalada da resposta • *Framework* NIST	Escalada da Resposta a ciberincidentes no NIST	Processos, Responsabilidades, Órgãos, Funções, Entidades, Grupos de tomada de decisão envolvidos na resolução de incidentes.	Análise documental
	OE2: Analisar a adequabilidade da estrutura, processos e responsabilidades previstos na nova LOEMGFA, na escalada de resposta a ciberincidentes.		**QD2:** De que forma a estrutura, processos e responsabilidades previstos na nova LOEMGFA, na escalada de resposta a ciberincidentes se encontram adequados?	• Ciberincidentes • Equipa de Resposta • Escalada da resposta	Escalada da Resposta a ciberincidentes nas FFAA		

Apêndice D – Metodologia

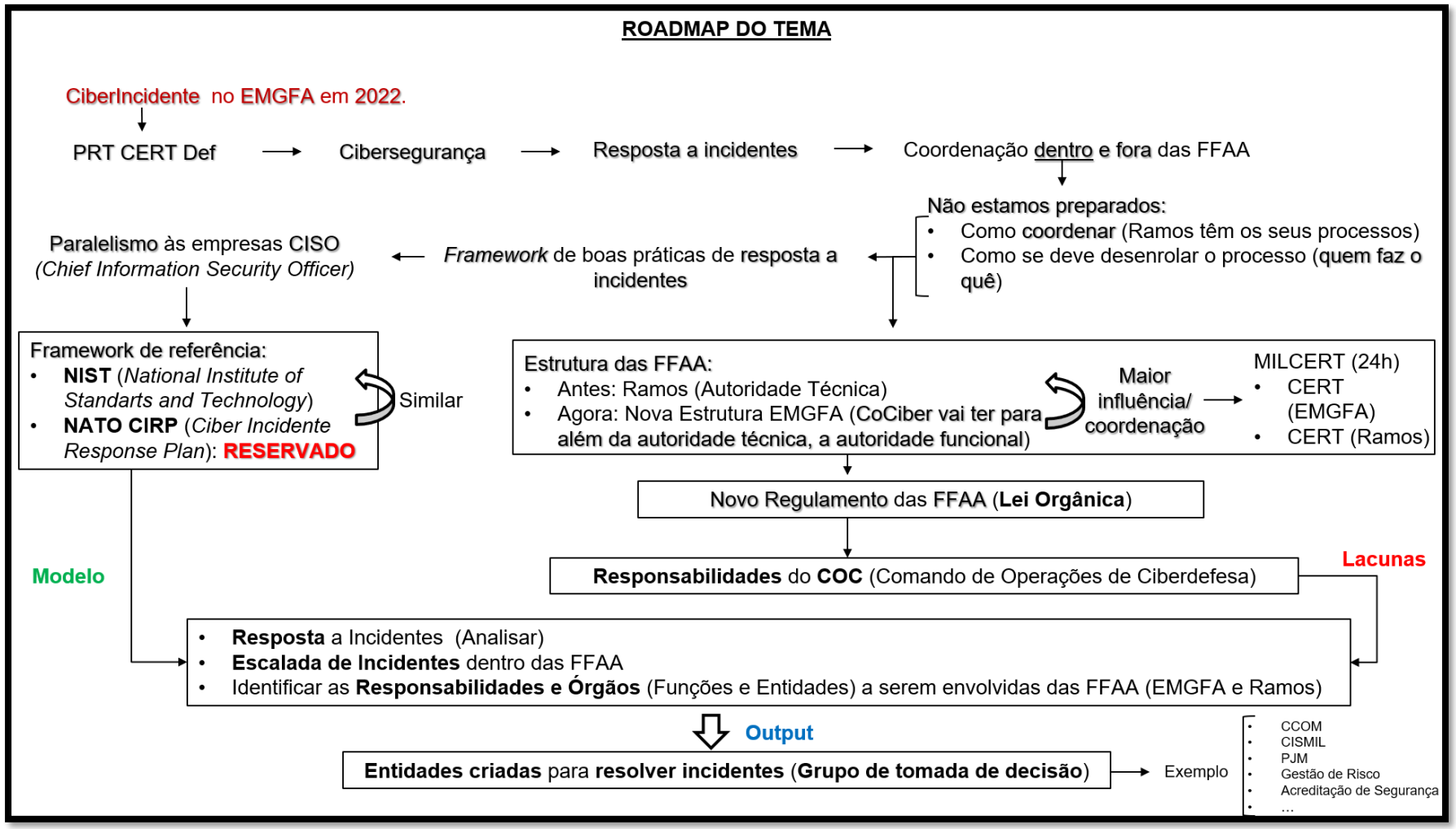


Figura 35 - Esquema sistematizado da metodologia (*Road Map do Tema*)

Apêndice E – Estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes

Quadro 3 - Estrutura, processos e responsabilidades existentes no NIST, na escalada de resposta a ciberincidentes

	PROCESSO	ESTRUTURA		ENTIDADES	RESPONSABILIDADES
	***Framework* NIST**				
Equipas de Resposta a incidentes	1) Fase da Preparação 2) Fase da Deteção e Análise 3) Fase da contenção, erradicação e recuperação 4) Fase Pós atividade do Incidente	Modelos Estruturais:	• Equipa de Resposta a Incidentes Central • Equipa de Resposta a Incidentes Distribuída • Equipa de Coordenação		
		Fatores para seleção do modelo da Equipa de Resposta:	• Necessidade de disponibilidade 24/7 • Equipa a tempo Integral *versus* tempo parcial • Moral dos funcionários • Custos • Especialização do pessoal		

		Composição das Equipas de Resposta:	• Funcionários	Chefe de Equipa (com 1 ou mais Adjuntos)	• Atuar como elo de ligação com a estrutura superior de gestão da organização e outras equipas e organizações (internas e externas), contruir relações de confiança e estabelecer meios de comunicação adequados: • Interno: - Direção - Gabinete de Assuntos Públicos - Departamento jurídico - Recursos Humanos - Outros CSIRT • Externo (documentar as interações com estas entidades): - CERT Nacional - Forças de Segurança - Outros CSIRT - Outras organizações afetadas por um incidente - Entidades com conhecimento especializado (ISP, TI, fornecedores de software) - Media - Clientes • Desativar situações de crise: - Priorizar o tratamento de incidentes. - Tomar decisões e definir os riscos aceitáveis. • Assegurar que a equipa tem o pessoal, os recursos e as competências necessárias (completar, formar e treinar a equipa). • Assegurar que as atividades de resposta a incidentes são executadas corretamente: - Criar políticas, planos e procedimentos de resposta a incidentes, com as interações internas e externas da organização. - Definir os níveis de autoridade das equipas de resposta a incidentes. - Definir pontos de transição e escalonamento no processo de gestão de incidentes. - Definir serviços a serem executados pela equipa de resposta a incidentes. - Definir medidas de desempenho. - Estabelecer e desenvolver normas, procedimentos e métodos de recolha, análise e comunicação de dados (tratamento e comunicação de incidentes). • Desenvolver um processo de Lições Aprendidas.

			Líder de Incidente	• POC principal para lidar com um incidente específico. • Responsável pelo tratamento do incidente. • Coordenar as atividades dos elementos que tratam o incidente. • Recolher informações dos elementos que tratam o incidente. • Fornecer atualizações de incidentes a outros grupos. • Assegurar que as necessidades da equipa são satisfeitas.
			Líder Técnico	• Assume a supervisão e responsabilidade final, pela qualidade do trabalho técnico da Equipa (pelas suas elevadas competências Técnicas e experiência)
			Membros da Equipa de Resposta a Incidentes	• Assegurar a monitorização contínua, segurança e proteção das redes, sistemas, aplicações e dados. • Executam atividades de administração de sistemas, administração de redes, programação, apoio técnico e deteção de intrusão. • Possuir uma boa capacidade de resolução de problemas, um pensamento crítico e saber trabalhar em equipa. • Possuir uma boa capacidade de comunicação e de escrita (pela necessidade de interagir, com uma grande variedade de pessoas, e elaboração de propostas e procedimentos). • Pelo menos um elemento, proficiente em cada área de tecnologia. • Alguns membros serem especializados em áreas técnicas específicas (deteção de intrusão de rede, análise de *malware* ou forense).
			Especialistas técnicos não pertencentes à equipa (temporariamente)	Apoiar a Equipa e efetuar recomendações de melhoria/partilha de conhecimento e experiência.
		• Parcialmente *Outsourced*	Igual ao modelo dos Funcionários	
		• Totalmente *Outsourced*	1 supervisor + 1 ou 2 reservas	

Outras entidades da Organização que apoiam as Equipas de resposta a incidentes		Comando/Direção	Gerência superior/direção	• Estabelecer a política de resposta a incidentes, o orçamento e o pessoal: - Definir uma estrutura, modelo e número de Equipas de resposta incidentes. - Definir requisitos e orientações para a comunicação externa de incidentes e partilha de informação. • Coordenar a resposta a incidentes entre as várias partes interessadas, minimizar os danos e informar as outras partes.
		Segurança da organização	Pessoal de segurança da informação	Apoiar certas fases de tratamento de incidentes (prevenção, contenção, erradicação e recuperação).
			Responsáveis pela segurança física e gestão de instalações	Permitir o acesso às instalações, durante o tratamento de incidentes.
		Departamento das Tecnologias da Informação	Técnicos das TI	Prestar apoio, pelas suas competências e pela melhor compreensão da tecnologia que gerem numa base diária, permitindo assegurar que sejam tomadas as medidas apropriadas para o sistema afetado.
		Departamento Jurídico	Peritos jurídicos (LEGAD)	• Rever os planos de resposta a incidentes, as políticas e os procedimentos, assegurando a sua conformidade com a lei. • Prestar apoio sempre que se avalie a possibilidade de um incidente ter ramificações legais (recolha de provas; a acusação de um suspeito; uma ação judicial; a necessidade de um memorando de entendimento - MOU), ou outro acordo vinculativo, que envolva limitações de responsabilidade para partilha de informação.
		Departamento de Assuntos Públicos	Assuntos públicos e relações com os media	Apoiar, caso exista, a necessidade de informar os meios de comunicação social e o público.
		Departamento de Recursos Humanos	Recursos humanos	Prestar apoio relativamente à administração de pessoal e disciplinar.
		Departamento de Planeamento e Avaliação	Profissionais pelo planeamento da continuidade do negócio	• Possuir o conhecimento do impacto dos incidentes. • Efetuar as avaliações de impacto empresarial, as avaliações do risco e a continuidade dos planos de operações. • Apoiar no planeamento da resposta a adotar.

Fonte: Adaptado a partir de NIST (2012)

Apêndice F –Enquadramento da lei orgânica (2022) do EMGFA

A Lei n.º 2/2021, que aprovou a Lei Orgânica de Bases da Organização das Forças Armadas, e a Lei Orgânica n.º 3/2021, ambas de 9 de agosto, que veio alterar a Lei de DN, aprovada pela Lei Orgânica n.º 1-B/2009, de 7 de julho, estabeleceram um novo paradigma estrutural da DN e das FFAA, reforçando o papel do CEMGFA e do EMGFA. Impondo a aprovação de uma nova orgânica do EMGFA para otimizar o funcionamento das FFAA, garantindo o princípio da unidade de comando, nomeadamente, através da passagem dos Chefes de Estado-Maior dos Ramos para a dependência do CEMGFA para todos os assuntos de natureza militar, cabendo ao CEMGFA a responsabilidade pelo cumprimento de todas as missões das FFAA (com exceção da busca e salvamento marítimo e aéreo). Estas circunstâncias, exigem do EMGFA a necessidade de coordenação dos assuntos de natureza conjunta, que envolvam os EM e os comandos de componente dos Ramos (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 3).

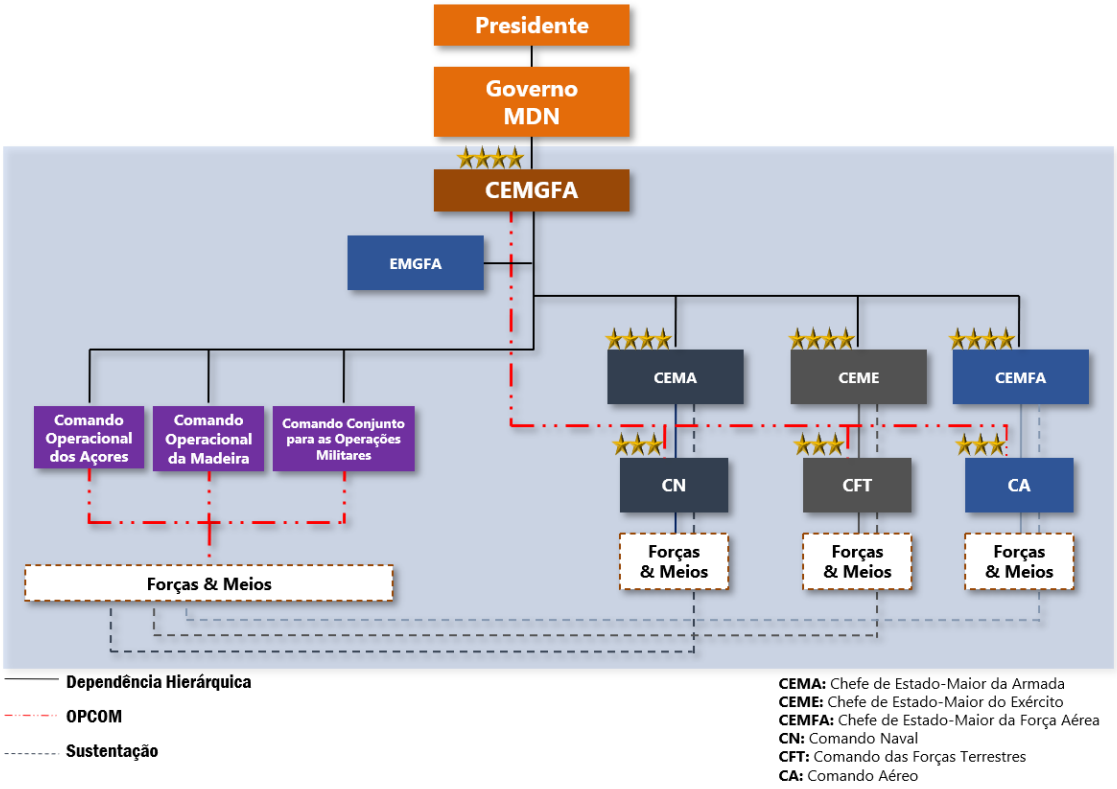


Figura 36 - Macroestrutura das FFAA

Fonte: Adaptado a partir de Briefing do CCOM ao Curso de Estado-Maior Conjunto 2022/23 (15 de abril de 2023).

O Decreto-Lei n.º 19/2022, de 24 de janeiro, veio estabelecer a nova LOEMGFA e alterar as Leis Orgânicas dos três Ramos das FFAA, reorganizando estas em função do produto operacional, privilegiando uma estrutura de forças baseada em capacidades conjuntas, assente num modelo de organização modular e flexível e com uma efetiva arquitetura de comando conjunto.

A organização do EMGFA baseia-se numa estrutura vertical e hierarquizada, em que os seus órgãos relacionam-se através de níveis de autoridade: hierárquica (é a linha de comando que estabelece a dependência de um órgão ou serviço, na estrutura das FFAA, em relação aos órgãos de comando), funcional (conferido a um órgão para superintender processos, sem incluir a competência disciplinar), técnica (permite a um órgão

fixar e difundir normas de natureza especializada, sem incluir a competência disciplinar) e de coordenação (conferida aos órgãos subordinados, a qualquer nível, para consultar ou coordenar diretamente com um comando ou entidades, dentro ou fora da sua linha de comando, sem incluir a competência disciplinar) (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 7).

O EMGFA passa a ser dotado de estruturas principais, distintas, o Estado-Maior Conjunto (para reforçar o apoio à decisão na prospetiva e planeamento estratégico, ao nível genético, estrutural e operacional) e o CCOM (para coadjuvar no comando das forças e meios em missões das FFAA, nos planos externo e interno). A missão do EMGFA:

> […] no âmbito do planeamento, direção e controlo, passa, também, a contemplar, para além do emprego das Forças Armadas em missões e tarefas operacionais, a estratégia de defesa militar, o ensino superior militar, a saúde militar, as informações e segurança militares, a **ciberdefesa**, os aspetos militares do programa espacial da DN e a inovação e transformação nas Forças Armadas. (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 3)

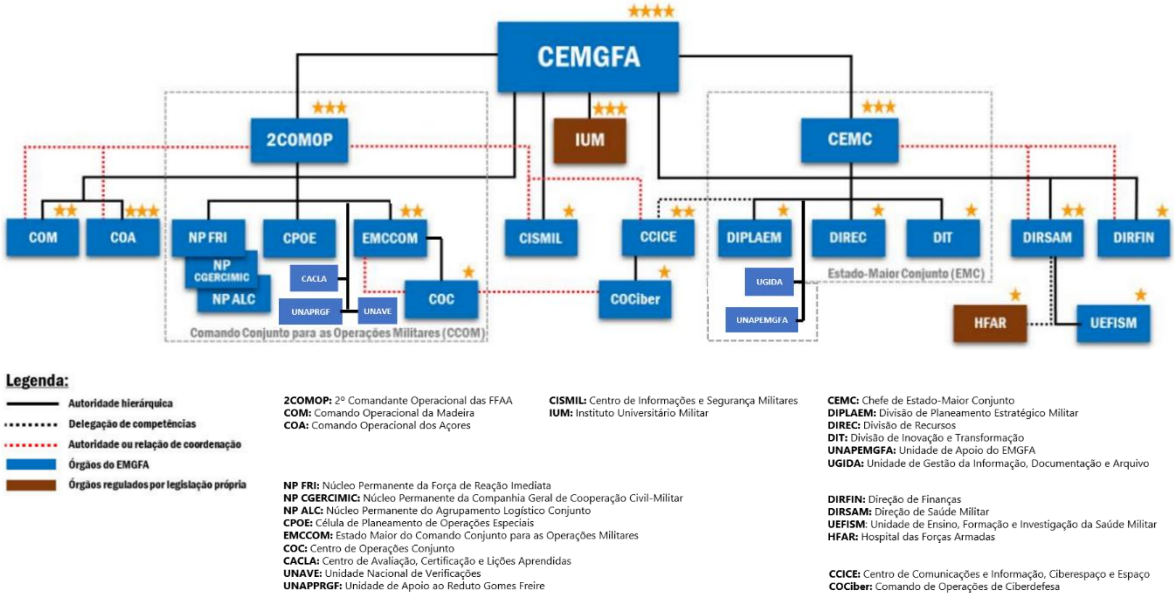


Figura 37 - Macroestrutura do EMGFA

Fonte: Adaptado a partir de Briefing do CCOM ao Curso de Estado-Maior Conjunto 2022/23 (15 de abril de 2023).

Face aos novos domínios das operações, entre eles o ciberespaço, é criado o CCICE (para habilitar a capacidade de comando e controlo conjunto das FFAA, e assegurar o exercício do comando de operações militares no e através do ciberespaço), na direta dependência do CEMGFA, como órgão de ciberdefesa, absorvendo as funções da anterior DCSI (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 23).

Apêndice G –Principais atribuições de algumas entidades das FFAA

Das atribuições do **CCICE**, realça-se (Decreto-Lei n.º 19/2022, de 24 de janeiro, p. 23):

- "Planear, coordenar, sustentar e executar as medidas de segurança […] e de resposta a incidentes para a proteção […] da infraestrutura tecnológica conjunta no âmbito das FFAA e […] MDN […]";
- "Assegurar o conhecimento situacional […] do ciberespaço […] nas FFAA, através de uma permanente partilha de informação";
- "Propor, planear, coordenar e conduzir operações militares no e através do ciberespaço […]";
- "Disponibilizar e coordenar a capacidade de ciberdefesa no emprego de forças e meios […] em missões de natureza operacional que sejam atribuídas aos ramos das FFAA, […] e em complemento das suas capacidades próprias";
- "Atuar em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, cibersegurança, cibercrime e ciberterrorismo […]";
- "Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques, no âmbito das FFAA e […] MDN".

Das atribuições do **COCiber**, destacam-se (EMGFA, 2021, pp. 2-4):

- "[…] assegura o exercício do comando operacional e tático das forças e meios de ciberdefesa das FFAA, no cumprimento das missões que lhe sejam atribuídas";
- "[…] tem a exclusividade da realização de ações com efeitos em infraestruturas externas às FFAA e constitui-se como o único ponto de contacto para a ciberdefesa nacional";
- "Planear o emprego e conduzir, ao nível operacional e tático, as operações no ciberespaço nos planos externo e interno";
- "Assumir a direção e coordenação da capacidade nacional de ciberdefesa";
- "Assegurar o controlo e o conhecimento situacional do ciberespaço nas FFAA";
- "Contribuir para o estudo e planeamento de soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço, no âmbito da cibersegurança setorial da DN;
- "Colaborar na investigação, recolha e salvaguarda de prova nos processos de análise de incidentes nas redes da DN, e dirigir e coordenar a análise e implementação de medidas de mitigação";
- "Atuar, ainda, em articulação e estreita cooperação e colaboração com as estruturas nacionais responsáveis pela cibersegurança e pelo combate à ciberespionagem, cibercrime e ciberterrorismo";
- "Partilhar a informação […] com os CIRC nacionais e internacionais, de forma articulada com as competências de coordenação da cooperação nacional e internacional do CNCS".

Das atribuições do **BTms**, do CTms do **Exército**, entre outras, assegura a ciberdefesa das forças em operações, nomeadamente através da (EME, 2016, p. 4):

- Gestão em CSI;

- Prevenção, deteção e recuperação de qualquer tipo de incidente/ataque contra os sistemas de informação táticos;
- Coordenação e investigação de incidentes e partilha de informações com o NuclCIRCEx.

Das competências da **DITIC** (na **Marinha**), destacam-se:

> […] Gerir, operar e manter a estrutura de segurança e defesa do ciberespaço e da informação na Marinha, assegurando a capacidade de resposta a incidentes no ciberespaço e de SegInf (CIRC) na Marinha, através de equipas próprias de combate às ameaças em computadores e em infraestruturas de redes (CERT ou CSIRT), disponibilizando processos e tecnologias que assegurem o adequado nível de segurança num contexto de gestão de risco. (EMA, 2016, p. 2)

Das competências da **DIVCSI, DCSI** e dos **Centros de Informática das Unidades** (na **Força Aérea**), destacam-se (FA, 2011, pp. 4-3 e 4-4; FA, 2013, p. 6-2):

- Elaborar a Política de Ciberdefesa da FA e mantê-la atualizada; coordenar a necessidade de intervenção dos Grupos de Reação a Incidentes de Segurança Informática (designados na altura por GRISI), no interior do ramo e no exterior, em sistemas conjuntos (DIVCSI).
- Providenciar e garantir a segurança das infraestruturas de rede, comunicações, sistemas e plataformas tecnológicas contra ataques no âmbito da ciberdefesa, assegurando confidencialidade, integridade e disponibilidade da informação (DCSI).
- Implementar os procedimentos locais estabelecidos pela DCSI (Centros de Informática das Unidades).

Apêndice H – Estrutura, processos e responsabilidades nas FFAA, na escalada de resposta a ciberincidentes

Quadro 4 - Estrutura, processos e responsabilidades nas FFAA, na escalada de resposta a ciberincidentes

PROCESSO	ESTRUTURA			ÓRGÃO/ENTIDADE	RESPONSABILIDADES
FFAA Portuguesas					
Da pesquisa bibliográfica e dos documentos analisados, não foi identificada nenhuma referência à existência de algum plano de reação a incidentes nas FFAA, nomeadamente para o escalar dos incidentes.	**EMGFA**	**Comando das FFAA**	Gabinete do CEMGFA	Gabinete do EMGFA.	• **Assessoria Jurídica** (presta apoio jurídico e contencioso, e conduz os assuntos de natureza jurídica, no âmbito das atribuições e competências do EMGFA). • **Relações Públicas** (assegura as atividades de comunicação, informação e relações-públicas do EMGFA).
		CCICE	• CCICE dispõe de autoridade técnica no âmbito das CSI, Guerra Eletrónica e SegInf; e dispõe de autoridade funcional e técnica no âmbito da ciberdefesa.	• Atualmente não existe um NCIRT na estrutura do EMGFA, mas está previsto futuramente a sua existência.	
		COCiber	• COCiber detém autoridade de coordenação com o CCOM, o CISMI e as estruturas internacionais ligadas à ciberdefesa e à cibersegurança cooperativa. • COCiber tem na sua dependência técnica e funcional o NCIRC do EMGFA e as componentes de ciberdefesa dos Ramos. • COCiber tem autoridade técnica com o NCIRC do MDN e o CDD.		

			Forças de Operações de Ciberdefesa (FOCiber)		• Garantir a **componente e suporte técnico às operações no ciberespaço**. • **Aconselhar o comando superior das soluções técnica**s mais adequadas para cumprir os **objetivos**. • Garantir a **constituição das Equipas das Forças de Missão** do Ciberespaço (EFMCiber).
				O PRTCERTDEF, é a entidade CSIRC coordenadora de todas as outras CSIRC da Defesa (**responsável pela direção técnica, monitorização e coordenação da resposta a incidentes das redes da Defesa Nacional**): • Chefe de Divisão. • Célula de Intel. • Célula de Vigilância e Deteção. • Célula de Análise Forense. • Célula de Reconhecimento e Antecipação • Célula de Resposta e Apoio Técnico ao Planeamento	• Chefe de Divisão (guarnecido pelos Oficiais Superiores, Capitães e Subalternos das FOCiber) define as prioridades de execução e garante a ativação das células necessárias para o cumprimento das tarefas definidas superiormente.• Célula de Intel (guarnecida por elementos da Secção de Informações Táticas) mantém a vigilância permanente das fontes de Intel, mantém informado o Chefe de Divisão e os elementos da célula de Vigilância e Deteção sobre informações relevantes.• Célula de Vigilância e Deteção (guarnecida por elementos das Secções de Defesa e de Resposta) mantém a vigilância permanente nas redes da defesa, reagindo aos eventos anómalos.• Célula de Análise Forense (guarnecida por elementos da Secção de Análise Forense) realiza investigações forenses aos eventos anómalos.• Célula de Reconhecimento e Antecipação (guarnecida por elementos do Núcleo de Exploração) asseguram o reconhecimento de sistemas ou redes digitais e executam medidas preventivas de proteção dos sistemas da Defesa ou penetração de alvos.• Célula de Resposta e Apoio Técnico ao Planeamento (guarnecida por elementos da Secção de Resposta) executam a resposta a eventos (e ações ofensivas se determinado superiormente); garantem o aconselhamento técnico no processo de planeamento e elaboram os planos técnicos para provocar os efeitos desejados por este.

			• Centro de Operações de Ciberdefesa (OPSCiber) (Efetua o planeamento, preparação, controlo, coordenação, condução e a avaliação das operações militares no ciberespaço).	• O *Battle Watch Captain* (BWC) e o *Intel Watchkeeper* (IWC).	• O BWC responsável pela reação a qualquer situação emergente ou incidente, e o IWC, para a atualização do panorama situacional das informações e a matriz de risco.
			• Estado Maior (EM)	• A C0 (Coordenação). • A C2 (Informações). • A C3 (Operações). • A C5 (Planos). • A C7 (Formação e Treino). • A C9 (Cooperação e Relações Externas).	• C0 para a **assessoria jurídica.** • C2 na identificação de ameaças para reduzir e mitigar o risco; e para analisar, processar e disseminar as informações. • C3 na **avaliação de impacto de efeitos;** coordenação dos esforços de mitigação com os responsáveis dos sistemas; e na manutenção do conhecimento situacional. • C5 na atualização do risco. • C7 no desenvolvimento do processo de **lições aprendidas**. • C9 para assegurar a **coordenação e cooperação interagências**, com o CNCS, o CERT Portugal, a PJ, o SIS, o CERT.PT e outros organismos nacionais.
			• Forças de Operações de Ciberdefesa (FOCiber)	• Núcleo de Conhecimento Situacional e o Núcleo de Exploração da Secção de Informações Táticas	• Desenvolver a **atividade ISR** • Identificar e classificar possíveis ataques futuros.
				• Secção de Defesa	• Garantir a operação das plataformas de **monitorização**. • Contribuir para o **esclarecimento situacional**. • Estabelecer a ligação com a os núcleos CIRC dos Ramos e coordenar a resposta a incidentes).
				• Secção de Resposta	• Executar ações de resposta a eventos de segurança nas redes. • Analisar vulnerabilidades.
				• Secção de Investigação Digital	• Efetuar perícias digitais especializadas e de engenharia inversa na área de **análise forense digital**.

			• Departamento de Sistemas de Ciberdefesa (DSCiber)	• Secção de Tecnologias de Ciberdefesa	• Assegurar a confidencialidade, integridade e disponibilidade da informação.
				• Secção de Auditorias e Análise de Vulnerabilidades	• **Gestão do risco e dos potenciais impactos nos sistemas das FFAA**. • **Propostas e avaliação das medidas de resposta ao risco** associadas às vulnerabilidades encontradas.
	Exército (DCSI - Direção de Comunicações e Sistemas de Informação)	**DCSI**	Na **nova reestruturação** das FFAA, a DCSI deixa de existir, passando as suas funções a pertencer à Direção de Comunicações e Informação (**DCI**).		
			A **estrutura CSIRC é distribuída** dentro da DCSI, entre o **NuclCIRCEx** e o **ModTACTCIRC** do **Centro de Transmissões**.	• Repartição de Sistemas de Informação • Repartição de Gestão da Informação e Conhecimento. • Repartição de Guerra da Informação.	
		Centro de Transmissões do Exército	Departamento de Operações de Comunicações e Sistemas de Informação	• **01 Equipa CIRC** (do Destacamento de Comunicações e Sistemas de Informação do Centro). • **01 Equipa CIRC** (do Destacamento de Comunicações e Sistemas de Informação do Norte).	
			Departamento de Ciberdefesa e Segurança da Informação	**Oficial Adjunto do Núcleo de Operações de Ciberdefesa**	**Cmdt do Módulo Tático CIRC**
			ModTatCIRC do **Batalhão de Transmissões**	• 01 **Seção Integradora** • 01 **Secção Ofensiva** • 01 **Secção Defensiva**	• **Recolher e partilhar informações** entre várias fontes e em tempo útil. • **Detetar incidentes/ataques**, efetuar a **avaliação** de entidades e de **situação.** • Prevenir, **mitigar** e por **fim** a um **ciberataque.** • Efetuar a **avaliação do risco** para uma operação (no âmbito CSI). • **Decidir as ações a implementar** em tempo útil.

		NuclCIRCEx		• **Comando do Núcleo** • **01 SecRespIncAnFor** • **01 SecWatchkeepIncHandlOf**	• Garantir a **resposta a incidentes de segurança e defesa** do ciberespaço do **Exército**. • **Coordenar com o COCiber na resposta** a incidentes de segurança, ao nível das **FFAA**. • **Trabalho colaborativo e integrado** com os restantes **NCIRC da Defesa**.
	Marinha (DITIC - Direção de Tecnologias e Comunicações)	**DITIC**	Tem uma estrutura CSIRT central (na DITIC), composta e articulada entre o Gabinete de Projetos, Normalização e Segurança (GPNS) e o NCIRT (chefiado em acumulação por um oficial do GPNS).	• GPNS • NCIRT	O GPNS articula-se com o NCIRC para efeitos de **análise do risco** e propostas de **medidas de mitigação de vulnerabilidades**.
				• Divisão de Administração e Sistemas e de Comunicações (DAC)/Secção de Administração de Redes (SAR) • Divisão de suporte aos Serviços e sistemas em Exploração (DSE).	Em situações de resposta a incidentes **reforça o GPNS/ETIR e o NCIRT**.
		GPNS	Equipa Técnica de Intervenção Rápida (ETIR)	**• ETIR-C (Oficial Coordenador da equipa).• ETIR-E (área da energia).• ETIR-M (área do MMHS).• ETIR-R (área das redes).• ETIR-S (área dos serviços).• ETIR-T (área das telecomunicações).**	Assegurar a **capacidade de resposta** adequada para a **resolução de incidentes** em áreas críticas, repondo os sistemas e serviços que afetem a capacidade operacional ou as missões em curso.
		NCIRC		• **Chefe do Núcleo CIRC**. • **01 Equipa Forense** (com 02 Analistas Forenses para as redes e sistemas). • **01 Equipa de Gestão de Incidentes** (com 03 Gestores de Incidentes e 06 Monitores de Incidentes).	• Garantir a **capacidade de resposta** a incidentes de segurança e defesa do ciberespaço e da informação. • Assegurar a **coordenação técnica** da resposta a incidentes de segurança da informação. • Assegurar a **colaboração, integração e coordenação com o COCiber e com os NCIRC dos Ramos** na resposta a incidentes de segurança ao nível das FFAA ou infraestruturas críticas nacionais. • **Partilhar informação** com os NCIRC nacionais e internacionais. • A **gestão e tratamento de incidentes, recolha de prova** e realização de **ações de investigação forense**.

	Força Aérea (DCSI)	**DCSI**	• A CSIRC na estrutura da DCSI não é claramente identificável, por se encontrar subordinada a uma Sub-Repartição. • A estrutura CSIRC é central, integrada na Repartição de Tecnologia de Informação da DCSI do Comando da Logística da Força Aérea (CLAFA)	**• Repartição de Sistemas de Informação (RSI)** **• Secção de Suporte a Sistemas de Tecnologias de Informação (SSTI)**	
		Repartição de Tecnologias de Informação (RTI)	Sub-Repartição de Segurança Informática e Ciberdefesa	**• Chefe de Secção.**	• Dirigir, coordenar e controlar a execução das tarefas da Secção. • Estabelecer normas e procedimentos de segurança dos Sistemas de Informação/Tecnologias de Informação (SI/TIC).
				• Analistas de Segurança de SI/TIC	• Elaborar as **normas técnicas de administração da infraestrutura** tecnológica. • Implementação e **monitorização das normas e medidas de segurança**. • **Monitorização dos sistemas de defesa** de perímetro e segurança da rede em geral. • Colaborar na **identificação e avaliação de soluções** técnicas. • Colaborar na **análise forense** de incidentes informáticos. • Assegurar a **capacidade de resposta** a incidentes.

LEGENDA:

Equipas de Resposta a Incidente
Outras entidades da Organização que podem apoiar a Equipa de resposta a incidentes

Apêndice I – Lacunas identificadas nas CSIRC do EMGFA e Ramos

Quadro 5 - Lacunas identificadas nas CSIRC do EMGFA e Ramos

CSIRC FFAA	LACUNAS IDENTIFICADAS	IND. / Severidade
EMGFA	• Atualmente não existe um CIRT na estrutura do EMGFA (está previsto futuramente a sua existência).	O/E
	• Não é claramente identificada:	
EMGFA/MAR /FA	○ A função do Líder de Incidente (enquanto POC responsável pelo tratamento de incidentes).	R
EMGFA/EXE/FA	○ A função do Líder Técnico.	R
EXE/MAR/FA	○ A função de assessoria jurídica.	R
EMGFA/EXE/MAR/FA	○ A função de assuntos públicos.	R
EXE/MAR/FA	○ A função de lições aprendidas.	R
EXE	○ A função de análise forense.	R
EMGFA/FA	○ A responsabilidade de gestão do risco.	R
MAR/FA	○ A responsabilidade de gestão da SegInf.	R
EMGFA/EXE/MAR/FA	○ A responsabilidade de definição dos pontos de transição e escalonamento no processo de gestão de incidentes.	P
EMGFA	• Sobreposição de tarefas nas FOCiber do COCiber, comparativamente ao PRTCERTDEF (provavelmente resultante de algumas das funções deste serem asseguradas em acumulação por elementos das Secções de Defesa e Resposta das FOCiber).	O/E
EXE	• A descentralização de pessoal e meios CIRC por diferentes entidades (Centro de Transmissões, BTms e NuclCIRCEx), incrementa a necessidade de controlo e coordenação.	EST
EXE	• A distribuição das várias entidades do ModTatCIRC por diferentes Órgãos (Departamento de Operações de Comunicação e Sistemas de Informação, Departamento de Ciberespaço e Segurança da Informação, e o BTms) dificulta a articulação dos meios, o controlo e coordenação.	EST
EXE/MAR/FA	• A estrutura da CIRT do Ramo tendo menos entidades (menos capacidade) comparativamente ao PRTCERTDEF, em conjunto com a necessidade e dependência de apoio de outros órgãos do Ramo (fora da sua capacidade de ciberdefesa) e do EMGFA (COCiber) (p. ex. para o apoio jurídico, assuntos públicos e para o planeamento, coordenação e avaliação da reação a incidentes), reduzem a eficácia da capacidade de tratamento do incidente ao nível do Ramo.	O/E
EXE/MAR/FA	• A existência de funções que não são ocupadas permanentemente na capacidade CIRT, reduz a eficácia da prevenção e tratamento de incidentes.	O/E
MAR	• A estrutura e articulação da CSIRC está bastante dependente da ETIR e outras divisões da DITIC (em acumulação de funções), nomeadamente para a parte técnica, dificultando a articulação dos meios, o controlo e coordenação.	EST
FA	• A CSIRC estar localizada hierarquicamente numa Sub-Repartição, dificulta a coordenação, gestão de incidentes, fluxo de informação e conhecimento e o poder de decisão.	EST

LEGENDA:	
IND: Indicador	**O/E:** Órgão/Entidade
P: Processo	**R:** Responsabilidade
EST: Estrutura	

Fonte: Autor (2023).

GRAU DE SEVERIDADE	
Catastrófico (I)	Perda de capacidade para cumprir a missão ou falhar o cumprimento da missão (...)
Crítico (II)	Degradação significativa (severa) na capacidade para cumprir a missão ou na prontidão da unidade (...)
Marginal (IV)	Degradação da capacidade de cumprimento da missão na prontidão da unidade (...)
Negligenciável (IV)	Pouco ou nenhum impacto negativo na operação (...)