CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NO CIBERESPAÇO UMA ABORDAGEM DOTMLPI-I

Paulo Jorge Baptista das Neves

Dissertação para a obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço

Mestrado em Segurança da Informação e Direito no Ciberespaço

Orientadores: Capitão-de-fragata (Doutorado) Fernando Jorge Ribeiro Correia
Professor Doutor Carlos Manuel Costa Lourenço Caleiro

Júri

Presidente: Professor Doutor Paulo Alexandre Carreira Mateus
Orientador: Capitão-de-fragata (Doutorado) Fernando Ribeiro Correia
Vogal: Professor Doutor Paulo Cardoso do Amaral
Vogal: Professora Doutora Raquel Alexandra Jesus Gil Martins Brízida

Julho 2015

Agradecimentos

Ao Centro Nacional de Cibersegurança na pessoa do seu coordenador o Dr. José Carlos Martins (Subdiretor Geral do Gabinete Nacional de Segurança) e do meu camarada eng. Gonçalo de Sousa que desde o primeiro contacto apoiaram esta colaboração e a muito importante participação do engenheiro Lino Santos (Coordenador do Departamento de Operações e Segurança do Centro Nacional de Cibersegurança) através do seu contributo numa entrevista escrita, cuja experiência e opiniões muito contribuíram para o resultado deste trabalho.

Ao engenheiro Gustavo Neves (Gestor de Serviços de Segurança na FCT-FCCN e ex-CERT.PT) pela partilha da sua experiência na organização e gestão de incidentes e pela disponibilidade para colaborar através de uma entrevista escrita, que se constituiu como peça fundamental para a realização deste trabalho.

Ao Capitão-Mar-Guerra Santos Coelho (Diretor de Serviços do Centro de Dados da Defesa) que através da sua participação numa entrevista escrita partilhou a sua opinião e experiência na área da Segurança, contribuindo com uma importante perspetiva operacional.

À Superintendência das Tecnologias de Informação da Marinha e à Direção de Tecnologias da Informação e Comunicações que, respetivamente na figura Sr. Contra-Almirante Superintendente e dos Srs. Diretor e Subdiretor me apoiaram para a realização este trabalho.

Ao Capitão-de-Fragata (Doutorado) Fernando Ribeiro Correia, orientador deste trabalho, que com o seu saber, disponibilidade, apoio e orientação contribuiu para o enriquecimento desta tese e me ajudou a navegar até bom porto.

À minha família e em especial à minha mulher Dulce, pelo seu grande apoio e exemplo de capacidade de trabalho e determinação.

Resumo

Ciberespaço, um espaço virtual onde cada vez mais se processam os mecanismos de luta pela supremacia da Informação. No entanto, apesar da sua natureza intangível, as ações que nele decorrem têm também tradução no plano físico, podendo comprometer infraestruturas que fornecem e controlam serviços críticos para a sociedade. Também no plano cognitivo os efeitos do que acontece no Ciberespaço afetam e influenciam as pessoas e a sociedade, nomeadamente através do controlo e manipulação da "opinião pública".

A sociedade em que vivemos é uma sociedade de informação, com comunicações omnipresentes quer a nível pessoal quer ao nível das instituições. Os Estados são cada vez mais dependentes das redes eletrónicas de comunicação, estando esta necessidade presente em todos os setores da sociedade e no próprio Estado, fazendo com que a Economia, os Serviços Básicos de apoio à Sociedade, a Banca e as Empresas entre outros, estejam dependentes de fluxos constantes de informação.

O Ciberespaço tornou-se assim valioso e crítico, levando naturalmente à sua utilização para a exploração de atividades ilícitas que ameaçam as pessoas, os seus bens a nível individual e à sociedade no seu todo. A Informação é sinónimo de poder, quem conseguir o seu controlo estará em condições de controlar muitos outros domínios críticos para o Estado e para a Sociedade. A importância de garantir a disponibilidade, a integridade e por vezes a confidencialidade da informação, impôs aos Estados a necessidade de organizarem a defesa do espaço virtual por onde circula toda esta informação.

Portugal começa agora a edificar estruturas que lhe permitam a implementação de capacidades de defesa do seu ciberespaço. Através do decreto-lei 69/2014 de 9 de maio o Governo aprovou a orgânica e os termos do funcionamento do Centro Nacional de Cibersegurança, dando assim resposta a uma recomendação da União Europeia para que cada estado membro implemente uma capacidade de resposta a incidentes de segurança cibernética.

Considerando a atualidade e a oportunidade relativamente à edificação destas estruturas de Cibersegurança e de Ciberdefesa, este trabalho pretende apresentar um modelo para a implementação de uma capacidade operacional de resposta e prevenção a incidentes de segurança da informação, seguindo a abordagem DOTMLPI-I[1] da Organização do Tratado do Atlântico Norte (OTAN) para a implementação de capacidades operacionais.

Palavras-chave: Ciberespaço, Cibersegurança, Ciberdefesa, Gestão de incidentes

[1] DOTMLPI-I - Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade

Abstract

Cyberspace, a virtual space where increasingly the mechanisms that struggle for Information supremacy are processed. However, despite its intangible nature, the actions that occurs in it also have translation on the physical world, being to compromise the infrastructures that provide and manage society critical services. Also on the cognitive level, the effects of what happens in Cyberspace affects and influences the people and the society nominated through the "public opinion" control and manipulation.

We live in an information society, with ubiquitous communications either at personal level or institutions level. Nations are each more and more dependent on electronic communication networks, with this need present in all sectors of the society and the State itself, causing that the Economy, the Society Basic Services support, Banking and Business among others, are dependent on permanent information flows.

Cyberspace has become thus valuable and critical, leading it naturally to its use for the exploration of illegal operations activities that threaten people, their individual property and the society as a whole. The Information is power, who gets its control will be able to control many other state and society critical domains. The importance of guarantee information availability, integrity and sometimes confidentiality, imposed to the States the need to organize their virtual space defence, through which all this information flows.

Portugal is now starting to build the structures that will allow it the implementation of defence capabilities of its cyberspace. Through Decree-Law 69/2014 of 9 May the government approved the structure and the terms of reference for the operation of the National Cyber Security Center, responding to a recommendation of the European Union so each state member have to implement a capability to respond against cyber security incidents.

Considering the present time and the opportunity concerning the construction of these Cyber Security and Cyber Defence structures, this paper aims to present a model for the implementation of an operational capability of information incident response and prevention of information security incidents, following the DOTMLPF-I [2] approach of the North Atlantic Treaty Organization (NATO) for the operational capabilities implementation.

Key words: Cyberspace, Cybersecurity, Cyber Defence, Incident management

[2] DOTMLPF-I – Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos e Siglas

CEMGFA – Chefe do Estado Maior das Forças Armadas

CERT – Computer Emergency Response Team

CLP – Controladores Lógicos Programáveis

CIICS – Cyber Information and Incident Coordination

CIRC – Computer Incident Response Capability

CNCS – Centro Nacional de Cibersegurança

CNA – Computer Network Attack

CND – Computer Network Defense

CNE – Computer Network Exploitation

CNO – Computer Network Operations

CSIRT – Computer Security Incident Response Team

DoD – Department of Defense

DOTPMLF-I - Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

ENISA – European Union Agency for Network and Information Security

FISMA – Federal Information Security Management Act

GNS – Gabinete Nacional de Segurança

GPL – General Public License

IDN – Instituto de Defesa Nacional

IDPS – Intrusion Detection and Prevention System

IP – Internet Protocol

IPS – Intrusion Prevention System

ISO – International Standard Organization

ITIL – Information Technology Infrastructure Library

MISP – Malware Information Sharing Platform

MN CD2 - Multi National Cyber Defence 2

NATO – North Atlantic Treaty Organization

NCIRC – NATO Computer Incident Response Capability

NCIRC-CC – NATO Computer Incident Response Capability Coordination Centre

NCERT – NATO Computer Emergency Readiness Team

NIST – National Institute of Standards and Technology

NTP – Network Time Protocol

OGC – Office for Government Commerce

OTAN – Organização do Tratado do Atlantico Norte

SCADA – Supervisory Control and Data Acquisition

SEGNAC – Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas

SGSI – Sistema de Gestão de Segurança da Informação

SIC – Sistema de Informação e Comunicações

SIEM – Security Information and Events Management

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicações

UPS – Uninterrupted Power Supply

US-CERT – United States Computer Emergency Readiness Team

Glossário

Backdoor – Tipicamente, software não autorizado e escondido ou um mecanismo de *hardware* utilizado para contornar os controlos de segurança. (CNSS, 2010)

Botnet – Uma *botnet* consiste num número grande de computadores que foram comprometidos e são usados para criar e enviar *spam*, ou vírus, ou alagar uma rede com mensagens que provoquem p.ex. um ataque de negação de serviço. (SANS, Glossary of Security Terms, 2015)

Ciberataque – Ato ou ação iniciada no ciberespaço para causar dano através do compromisso das comunicações da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas. (NATO, NATO Cyber Defence Taxonomy and Definitions, 2014)

Ciberdefesa – Os meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações, da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas. (NATO, NATO Cyber Defence Taxonomy and Definitions, 2014)

Ciberespaço – Um domínio global e virtual criado pela interligação de todas as redes de Comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas. (NATO, NATO Cyber Defence Taxonomy and Definitions, 2014)

Cibersegurança – Estratégia, política e normas com vista à segurança das operações no ciberespaço, abrangendo missões de redução da ameaça, de vulnerabilidades, de compromisso internacional, de resposta a incidentes, resiliência, e políticas de recuperação, incluído operações em rede, garantia da informação, ações judiciais, diplomáticas, militares e de inteligência relacionadas com a segurança e estabilidade da infraestrutura global de informação e Comunicações. (NICCSN, 2015)

COMPUSEC – Segurança de computadores. Aplicação de funcionalidades de segurança ao nível do *hardware*, *software* e *firmware* num sistema de modo a prevenir ou protegê-lo contra exposição, manipulação, modificação da informação ou negação de serviço. (ACO, 2006)

COMSEC – Segurança das comunicações. Aplicação de medidas de segurança às telecomunicações de modo a negar o acesso não autorizado a informações de valor, que possa decorrer da posse ou análise dessas telecomunicações ou para garantir a sua autenticidade. Tais medidas incluem criptografia e segurança das transmissões e emissões. (ACO, 2006)

Defacement – Desfiguração ou alteração de páginas web, usualmente feita como forma de protesto ou *hacktivismo*

EMSEC – Segurança das emissões resultantes da irradiação dos sistemas de informação e comunicações. (ACO, 2006)

Evento – Uma ocorrência num sistema, serviço ou rede indicando uma possível quebra de segurança da informação, política ou falha de controlos, ou uma situação desconhecida que poderá ser significativa em termos de segurança. (NIST N. I., 2013)

Incidente – Uma ocorrência que coloca em risco a confidencialidade, integridade ou a disponibilidade dum Sistema de Informação ou dos seus processos, armazenamento ou transmissão, ou que constitua

uma violação ou ameace vir a violar das políticas de segurança, procedimentos de segurança ou as políticas em vigor. (NIST N. I., 2013)

INFOSEC – Proteção dos sistemas de informação contra o acesso não autorizado ou modificação da informação armazenada, processada ou em trânsito, preservando a sua confidencialidade, integridade e disponibilidade. (ACO, 2006)

Macro – Conjunto de comandos e instruções, agrupados como um único comando, para realizar uma tarefa automaticamente. Esta funcionalidade permite escrever vírus sob a forma de macros e inseri-los em documentos, de modo a que estes sejam executados logo na abertura do documento.

Malware - *Software* ou *firmware* que se destina a executar processos não autorizados que terão um impacto adverso na confidencialidade, integridade, ou disponibilidade num Sistema de Informação. Um vírus, um *worm*, ou outra estrutura de código que infecte uma máquina. *Spyware* e algumas formas de *adware* são exemplos de código malicioso (NIST N. I., 2013)

Overflow – Uma condição de entrada de dados que permite que sejam introduzidos dados ou colocados em memória, para além da capacidade reservada para o efeito, provocando a escrita "por cima" de outra informação. Os atacantes exploram esta vulnerabilidade para bloquear um sistema ou para introduzir código especialmente escrito de modo a dar-lhes o controlo sobre o sistema. (CNSS, 2010)

TRANSEC – Segurança da transmissão. Componente da segurança das comunicações que resulta de todas as medidas, exceto as físicas, designadas para proteger as transmissões de interceções ou exploração não autorizada, por outros meios que não a criptografia. (ACO, 2006)

Vírus – Um programa de computador que pode copiar-se a sis próprio e infetar um computador sem conhecimento do utilizador. O vírus pode corromper ou apagar dados no computador, utilizar programas de *e-mail* para se espalhar a outros computadores, ou mesmo apagar tudo no disco rígido. (CNSS, 2010)

Vulnerabilidade dia-zero – Exploração de uma vulnerabilidade que aproveita a vantagem de ainda não existir nenhuma atualização de segurança (patch) disponível para essa vulnerabilidade. (NCSC, 2014)

Worm – Um programa auto-replicante, que se auto-propaga utilizando mecanismos da comunicação em rede. (CNSS, 2010)

1. Introdução

1.1. Ciberespaço

A palavra Ciberespaço foi utilizada pela primeira vez pelo escritor de ficção científica William Gibson em 1982[3] para descrever um espaço virtual sustentado na interligação em rede de máquinas e pessoas à escala global, definindo-o como um "mass consensual hallucination of computer networks"[4].

Na verdade, mesmo considerando a distância temporal que nos separa da capacidade visionária de Gibson em 1982, ainda hoje podemos definir o Ciberespaço como sendo um universo virtual criado pela interligação de computadores à escala planetária, que permite a ubiquidade e a omnipresença dos seus habitantes (utilizadores da rede) através da supressão da noção espácio temporal. André Matias e Rogério Bravo (2010) no seu artigo sobre o ciberespaço "Geopolítica, geoestratégia e ciberespaço: Notas introdutórias" mencionam que *os vetores espaço, tempo e caminho percorrido para se movimentar de um ponto para o outro, praticamente desaparece*. No entanto, apesar da sua natureza virtual, este espaço eletrónico de comunicação não deve ser encarado displicentemente, pois o Ciberespaço é tão real como os seus efeitos.

A vantagem de poder chegar instantaneamente a todo o lado, a independência dos fusos horários, levou a que também os Estados e as Empresas utilizem o Ciberespaço como base para as suas infraestruturas de comunicações, não só entre si, mas também como rede de suporte ao comando e controlo das suas infraestruturas, muitas das quais prestam serviços críticos à sociedade.

Sendo então este um espaço construído na interligação de várias redes de telecomunicações, de computadores e controladores, onde virtualmente todos os sistemas têm o potencial de comunicar entre si, é com naturalidade que vemos a transposição para esta realidade de todas as qualidades e defeitos da natureza humana. Através do Ciberespaço tanto podemos assistir ao lançar quase instantâneo de uma campanha global para auxílio a uma comunidade vítima de uma catástrofe natural, como a um ataque cibernético que poderá prejudicar uma empresa e a vida das pessoas que dela dependem. De acordo com um relatório da Europol que reflete sobre a utilização da Internet para atividades criminosas, existem mais de 2,8 mil milhões de utilizadores e mais de 10 mil milhões de terminais de acesso à internet (EC3, 2014). O Ciberespaço é assim uma realidade complexa onde interagem diferentes dimensões da sociedade e onde o valor maior reside na qualidade da informação que nele circula, seja na comunicação entre pessoas, entre organizações ou mesmo nas comunicações de comando e controlo de sistemas críticos. Este é um espaço virtual cujos acontecimentos se repercutem no mundo físico, tornando-se assim um problema global.

A perceção da criticidade deste Ciberespaço levou os militares a reconsiderar os tradicionais conceitos de operações. Em 2010 o Exército americano publicou um estudo estratégico sobre o conceito de operações no ciberespaço, onde caracterizou o ciberespaço dividido em três camadas distintas, uma camada Física, uma Lógica e uma camada Social, sendo estas constituídas por cinco

[3] William Gibson lançou o termo Ciberespaço num conto chamado "Burning Chrome", publicado na revista Omni. O termo viria a ser popularizado mais tarde após a publicação do seu famoso livro "Neuromancer" publicado em 1984.

[4] WIKIPEDIA, (Wikipedia, William Gibson, s.d.)"William Gibson", http://en.wikipedia.org/wiki/William_Gibson (consultado em outubro 2014)

componentes que são a Geográfica, a Rede Física, a Rede Logica, as Pessoas e as Ciber Pessoas (USArmy, 2010) aqui representados na figura 1.

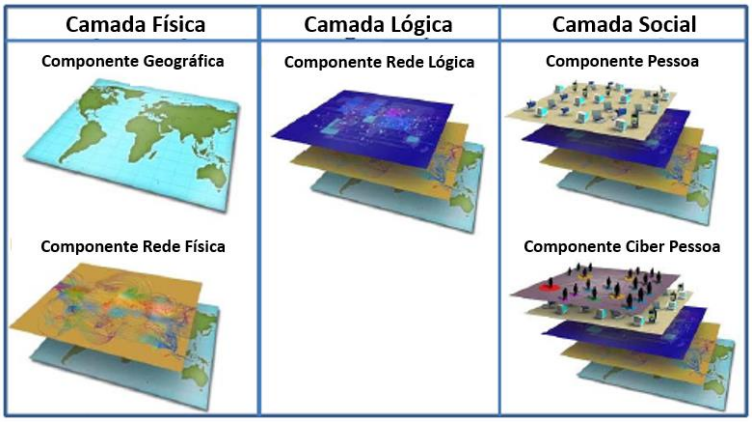

Figura 1 - Ciberespaço, 3 camadas, 5 componentes in, TRADOC Pamphlet 525-7-8 *(USArmy, 2010)*

A camada Física representa as redes físicas de computadores e sistemas, tendo em consideração a sua localização geográfica (duas componentes). Este aspeto é bastante relevante pois apesar de no Ciberespaço as fronteiras físicas pouco ou nada significarem, a realidade é que existe sempre uma ligação ao mundo Físico onde se encontram instalados os componentes da rede (*routers*, *switchs*, servidores, transmissores) nos quais assentam a abstração virtual do espaço (camada lógica).

A camada Lógica é constituída pelas ligações lógicas que são estabelecidas entre os vários nós da rede. Esta componente sendo essencialmente técnica permite a ligação de componentes tão distintos como sejam os computadores, *tablets*, *smartphones* ou outros equipamentos que tenham o seu endereço IP[5] na rede.

A camada Social inclui os aspetos humanos e cognitivos e faz a separação entre a pessoa física e a pessoa ciber. Nesta ultima são consideradas as características que definem a pessoa enquanto elemento integrado na rede através de uma identificação (endereço de email, endereço IP, nome de utilizador) ou enquanto pessoa utilizadora dos serviços da rede (diversos perfis de utilização). É importante ter em consideração que cada pessoa pode ser várias ciber pessoas na rede (diversos perfis de utilização).

O estudo do Exército Norte Americano já mencionado conclui que o Ciberespaço consiste em muitos nós e redes diferentes interligados de forma crescente entre si. Apesar da sua característica virtual, que não segue o tradicional conceito de fronteira geográfica, continua a ser possível ser segmentado através da configuração direta das redes, dos protocolos e/ou através de mecanismos de cifra e *firewall*, criando organismos que se agrupam sob domínios distintos, como por exemplo ".gov", ".edu" ou ".com". Esta segregação por domínios permite criar um espaço multidimensional de espaços com alguma autonomia no Ciberespaço.

[5] Endereço IP é o número que identifica univocamente qualquer equipamento dentro da sua rede, eg: computador, impressora.

O estudo conclui ainda que este conceito multidimensional do ciberespaço e a sua ligação aos sistemas críticos da sociedade, bem como a necessidade de proteger a qualidade da informação, levou a que este espaço virtual seja identificado como um quinto domínio de guerra, tal como o Mar, a Terra, o Ar e o Espaço. Porém, o Ciberespaço surge como um domínio que permite a interdependência entre todos os outros domínios, através da existência de nós do Ciberespaço em todos eles (ver fig. 2).

Figura 2 - Ciberespaço, o quinto domínio de guerra

1.2. Um novo espaço de guerra

Em 1984, Fred Cohen apresentou pela primeira vez uma definição de vírus informático, como sendo *um programa que pode infetar outros programas modificando-os de modo a possivelmente incluir uma cópia evoluída de si mesmo* (Cohen, 1984). O processo de réplica para outros programas permite ao vírus uma capacidade de difusão, infetando programas noutros computadores, seja através de suportes de informação amovíveis, da rede de comunicações ou de serviços associados como por exemplo o correio eletrónico.

Quando Fred Cohen começou a falar de vírus informáticos, estes estavam ainda muito dependentes da intervenção humana para se conseguirem difundir, nomeadamente através da distribuição ou partilha de *disketes* entre os utilizadores. Quando os computadores começaram a comunicar em rede, primeiro dentro de pequenas intranets corporativas como por exemplo as redes do Estado e das universidades, depois em larga escala através da Internet, chegando a um público-alvo muito mais vasto, os vírus evoluíram para utilizar as grandes vantagens proporcionadas por uma rede de comunicações global. Desta forma conseguiram propagar as infeções a um ritmo superior ao observado até então. Hoje em dia os meios mais comuns de propagação de *malware*[6] são os serviços disponibilizados na rede, como sejam a navegação Web e o correio eletrónico, sendo comumente assumido que a grande "fonte" de vírus é a Internet.

O uso pessoal de computadores começou a massificar-se nos anos 80 e quase como uma consequência natural, alguns programadores começaram a produzir código que não tinha outro objetivo que não deixar a sua marca pessoal. Um exemplo destes primeiros programas que pelas suas

[6] *Malware* surge da aglutinação dos termos *Malicious Software* e hoje é utilizado como termo genérico que engloba todos os tipos de programas escritos com a intenção de algum modo comprometer um sistema informático eg: Vírus, Worms, Scripts e outros.

caraterísticas de replicação autónoma podemos classificar de vírus, surgiu no ano de 1986 e ficou conhecido por Brain. Tornou-se notado quando em 1987 os utilizadores da universidade de Delaware começaram a verificar que o nome do volume das suas disquetes era alterado de forma autónoma para "© Brain". Este era um vírus inofensivo, no sentido que não destruía a informação, limitando-se a alterar o nome do volume e a replicar-se (Paquette, 2010).

No final dos anos 90 a evolução dos "programas de escritório" da Microsoft levaram à popularização de programas como o Word e o Excel, que entre muitas novas capacidades apresentavam a possibilidade de correrem Macros[7]. Esta funcionalidade foi aproveitada para a criação de um dos primeiros vírus que teve impacto a nível global, o Melissa. Quando um utilizador abria um documento infetado com esta macro, o vírus recorria ao Outlook e enviava uma cópia do documento infetado para 50 pessoas da lista de contactos do utilizador[8]. O impacto deste vírus foi devastador pois criou uma reação em cadeia de envio e receção de mensagens de correio eletrónico, levando a um aumento desmesurado do volume de tráfego, acabando por tornar inoperacional este serviço em milhares de empresas privadas e estatais, com graves consequências económicas e operacionais para as mesmas.

Terminada a "era da inocência", nos anos seguintes continuaram a aparecer outros vírus cada vez mais sofisticados e perigosos. Em 2001 o vírus "I Love You" não só utilizava o correio eletrónico para se propagar, como também os então populares canais de Chat. Terá sido também dos primeiros a explorar deliberadamente as vulnerabilidades humanas ao nível do utilizador, ao escrever no assunto da mensagem, que esta era uma carta de amor de um admirador secreto. O impacto deste vírus foi estimado num prejuízo de mais de 10 mil milhões de dólares (Strickland, 2008). 2001 foi também o ano do aparecimento do vírus Code Red e das suas variantes, que ao contrário dos anteriores, explorava vulnerabilidades do sistema operativo (Windows 2000 e NT), permitindo um ataque de OverFlow[9]. A primeira versão deste vírus permitiu provocar um ataque de negação de serviço à Casa Branca, ao provocar o *crash* dos seus servidores por excesso de tráfego de acesso gerado pelo vírus. A segunda versão criava um *backdoor*[10] que permitia o acesso não autorizado aos servidores. Ainda nesse ano, aparece o vírus Nimda, explorando um *backdoor* criado pelo Code Red II, tonando-se o vírus que mais rapidamente se conseguiu espalhar pelas redes e sistemas, ao explorar simultaneamente várias formas diferentes de infeção. O seu principal objetivo era atacar os servidores da rede levando à sua indisponibilidade (Strickland, 2008). Nos anos seguintes surgem outros vírus que são não só mais sofisticados na sua forma de atuação e ocultação, como também começam a explorar vulnerabilidades noutras plataformas de interação com os utilizadores. São exemplo desta evolução o vírus SQL Slammer em 2003[11], que provocou uma situação de "negação de serviço" na Internet ao conseguir

[7] Uma Macro é um conjunto de comandos que pode ser armazenado e posteriormente executado pelo utilizador como um todo.
[8] http://www.symantec.com/security_response/writeup.jsp?docid=2000-122113-1425-99&tabid=2 (consultado em 01/11/14)
[9] Overflow é uma vulnerabilidade de segurança no código que permita escrever para além da área de memória prevista, corrompendo o programa inicial. Pode levar à sua interrupção imediata ou a adulterar os dados ou mesmo a introduzir código malicioso. (Correia, 2010)
[10] Uma alteração no programa inicial, permitindo o acesso não autorizado ao sistema com privilégios de administração.
[11] https://ethics.csc.ncsu.edu/abuse/wvt/Slammer/study.php, consultado em 02/11/2014

infetar mais de 75000 computadores via internet em apenas 10 minutos, explorando uma vulnerabilidade desconhecida no software SQL Server da Microsoft através de um ataque de Buffer Overflow. Nos anos seguintes vírus como o Sasser, o NetSky ou o Storm Worm[12] vieram colocar em evidência que mesmo tendo os sistemas de antivírus atualizados e os sistemas operativos com todas a correções do fabricante instaladas, a segurança dos sistemas passa também por ter políticas de segurança que enquadrem as ações dos utilizadores e talvez o mais importante, a construção de uma consciência global de segurança cibernética.

Nos exemplos apresentados anteriormente sobre alguns dos principais vírus que surgiram até ao ano de 2006, apresentando estes diferentes graus de sofisticação e autonomia, ou de serem dirigidos à exploração de vulnerabilidades específicas de determinados programas ou sistemas operativos, podemos afirmar que todos eles afetam em maior o menor grau, toda a comunidade de utilizadores, independentemente de quem estes sejam. Em 2007, pela primeira vez houve um ataque de larga escala dirigido não à internet no seu todo, mas a um conjunto específico de redes de computadores que tinham em comum pertencerem a um mesmo país.

A Estónia em 2007, alegadamente na sequência de uma situação de conflito com a sua minoria russa, foi vítima de um ataque massiço de *defacement* [13] e de negação de serviço aos servidores do Estado e de várias empresas, afetando principalmente as comunicações eletrónicas do Estado, da Banca e das Empresas mais representativas na economia do país. Sendo a Estónia um país que aposta fortemente na governação eletrónica e pioneira na otimização dos processos administrativos baseada na utilização das tecnologias de informação no Estado (cartão do cidadão, votação eletrónica, etc.), assenta a grande maioria das suas transações económicas e da sua atividade de governação pública e privada nos meios eletrónicos, nomeadamente na Internet e nas comunicações móveis. Estes ataques prolongaram-se por quase dois meses, provocando uma paralisia económica de consequências extremamente graves para o país. A Estónia não estava preparada para responder a este tipo de ataque e não possuía defesas nem mecanismos de recuperação e continuidade de negócio que lhe permitissem mitigar os efeitos destas ações.

Em 2008, um conflito interno na Geórgia com a comunidade separatista de origem russa na província da Ossétia do Sul e na Abcásia, levou à intervenção armada das forças russas em território georgiano. Durante o conflito armado que se seguiu, à semelhança do tinha acontecido na Estónia no ano anterior, as páginas do governo da Geórgia na Internet e as suas redes de telecomunicações, incluindo as redes móveis, estiveram sob um forte ciberataque de negação de serviço que provocou a indisponibilidade de vários serviços, antes e durante o conflito armado.

O resultado destes ataques cibernéticos à Estónia e à Geórgia, os primeiros conhecidos ao nível de todo um país, levou a que a segurança da informação e a proteção das infraestruturas críticas passassem a ser consideradas numa nova perspetiva, “o Estado terá de garantir não só a utilização segura do ciberespaço aos seus cidadãos como a salvaguarda da própria soberania” (IDN, 2013).

[12] O Storm Worm viria também a ser utilizado na propagação de BotNets (redes de computadores “zombies” que executam ações sob o controlo remoto de um hacker, sem conhecimento do seu proprietário) ao infetar computadores como o *malware* (Bot) que colocava o computador sob o poder do *hacker*. Esta poderosa forma de ataque permite entre outros a realização de campanhas de Spam ou de ataques de negação de serviço distribuídas.
[13] Desfiguração ou alteração de páginas web, usualmente feita como forma de protesto ou *hacktivismo*.

Em 2010 o mundo toma conhecimento da primeira ciber arma da história, criada especificamente para ataque a infraestruturas físicas. O Stuxnet foi uma peça de malware muito sofisticada que possuía a capacidade de reprogramar os Controladores Lógicos Programáveis (CLP) do sistema de SCADA[14] responsável, entre outras coisas, pelo controlo da velocidade de rotação das centrifugadoras de urânio do Irão. Através de um complexo sistema de Comando e Controlo idêntico ao utilizado pelas Botnets, e explorando várias vulnerabilidades de dia-0 dos sistemas operativos dos computadores, foi possível aos atacantes reprogramar os CLP das centrifugadoras iranianas, alterando a sua velocidade de rotação de modo que levasse à sua destruição ou inutilizando o urânio em processamento, ao mesmo tempo que controlava o sistema de monitorização e alerta da central iraniana, para que a monitorização remota mostrasse uma situação de normalidade. O impacto deste ataque, alegadamente por parte de Israel, provocou um atraso superior a 1 ano no programa nuclear do Irão e avultados prejuízos económicos (Langner, 2013).

Os exemplos anteriormente apresentados de situações ocorridas na Estónia, na Geórgia e no Irão, mostram inequivocamente a evolução para uma nova realidade, a da utilização do ciberespaço como um novo espaço de guerra, com as suas próprias ciber armas que permitem atingir alvos selecionados.

Mas a utilização do ciberespaço como espaço de guerra não está confinado às ações de ataque e sabotagem das infraestruturas criticas. Baseado nos princípios que levaram ao desenvolvimento do Stuxnet, nos últimos anos têm surgido novas armas cibernéticas cada vez mais sofisticadas, desta vez dirigidas não às infraestruturas criticas das nações, mas a um recurso igualmente crítico, a Informação.

O DuQu[15] em 2011, o Flame[16]e o Gauss[17] em 2012 aparecem como algo mais do que peças muito sofisticadas de *malware*, eles são parte integrante de complexos sistemas cibernéticos de inteligência que têm por objetivo principal o roubo de informação aos níveis superiores de decisão das organizações, constituindo-se assim como ciber armas de espionagem de grande valor para as redes de inteligência militar e industrial.

Por fim, como dizia Kevin Mitnik, um dos mais célebres *hackers* de todos os tempos, não podemos esquecer que *o elo mais fraco da segurança são as pessoas* (Mitnik & Simon, 2002). Baseado nesta realidade, em 2014 assistimos um novo tipo de ataque de ciber espionagem, dirigido a chefes militares, diplomatas e congressistas dos Estados Unidos. Baseando-se em contas fictícias de redes sociais, foram criadas relações de confiança com as vítimas que as levaram a instalar "voluntariamente" o *malware* de exfiltração nas suas máquinas. Este tipo de ataque, alegadamente perpetrado pelo Irão e que utiliza uma mistura de *malware* sofisticado com engenharia social, foi batizado de "Newscaster". (Lenon, 2014)

Os exemplos anteriormente apresentados mostram que estamos sem dúvida num novo espaço de guerra. Em 2014, na cimeira da OTAN em Gales, a aliança reconhece as ameaças emergentes do

[14] Supervisory Control and Data Acquisition (SCADA) é um sistema de gestão e supervisão industrial largamente utilizado em todo o mundo que permite o controlo de máquinas industriais a partir de sistemas de computadores (eg: gestão e monitorização a partir de um computador de uma rede de distribuição de energia elétrica).
[15] http://www.symantec.com/connect/ w32_duqu_precursor_next_stuxnet, consultado em 02/11/14)
[16] http://www.symantec.com/ connect/blogs/flame-most-powerful-malware-till-date, consultado em 02/11/14)
[17]http://www.symantec.com/connect/blogs/complex-cyber-espionage-malware-discovered-meet-w32gauss, consultado em 02/11/14)

Ciberespaço e assume a responsabilidade da defesa das suas próprias redes, garantindo a solidariedade para com os aliados, mas não descartando destes a responsabilidade de cada estado ter de possuir uma capacidade própria de proteção das suas redes nacionais (NATO, Wales Summit Declaration, 2014). No ponto 72 da referida declaração, a OTAN assume que a Ciberdefesa é parte integrante de uma defesa coletiva. No caso de um ciberataque a um estado membro que coloque em causa a "prosperidade, a segurança e estabilidade" do estado ou das relações Euro-atlânticas, este poderá levar à evocação do artigo 5º do Tratado do Atlântico Norte, levando a que o ataque seja considerado como sendo dirigido a toda a aliança[18], sendo esta ação analisada caso a caso.

Nesta cimeira a OTAN assume como prioridade o investimento na melhoria da Cibersegurança das redes nacionais dos estados membros, pois estas são parte integrante das infraestruturas de rede utilizadas pela aliança. Aposta também na integração da Ciberdefesa nas operações militares e no desenvolvimento das ações de educação e treino, aprofundando as parcerias com a União Europeia e a Industria, aproveitando as inovações tecnológicas e o conhecimento especializado do setor privado, de modo a atingir os objetivos de uma melhorada política de Ciberdefesa.

1.3. Organização para a segurança e defesa do Ciberespaço e da Informação

Sendo então a segurança do Ciberespaço vital para a garantia da qualidade da informação, que como vimos poderá ter impacto ao nível dos serviços básicos para o funcionamento da sociedade ou mesmo da soberania do país, estando este sujeito a ameaças que tanto poderão ter origem em atos de protesto social, ou com objetivos de natureza criminosa ou mesmo de guerra, compete primariamente aos governos dos países a organização para a segurança e defesa deste espaço. Esta organização pode ser subdividida em duas grandes áreas de intervenção, a Ciberdefesa e a Cibersegurança.

Na figura 3 apresenta-se uma visão gráfica de uma perspetiva sobre a relação entre alguns dos mais populares Cibertermos, relacionados com o objetivo de garantir a integridade dos Sistemas de Informação e Comunicações (SIC), de modo a garantir a qualidade da Informação para que esta esteja protegida, seja confiável e esteja disponível sempre que necessária.

[18] http://www.fd.uc.pt/CI/CEE/OI/NATO/Tratado_NATO.htm, consultado em 09/11/2014

Figura 3- Conceito de Segurança da Informação num ambiente de segurança SIC[19]

Num contexto de SIC, quando falamos de Segurança referimo-nos fundamentalmente a três aspetos essenciais, a segurança física das instalações e dos espaços operacionais, a segurança relativa ao pessoal que trabalha e manipula informação classificada ou sensível e finalmente a segurança do material que suporta a informação.

O termo INFOSEC resulta da agregação de duas disciplinas fundamentais da segurança da Informação, o COMSEC e o COMPUSEC. Enquanto o COMSEC se aplica à segurança das comunicações, nomeadamente à segurança da sua transmissão (TRANSEC), a proteção das suas emissões (EMSEC) e a parte de garantia da privacidade e integridade através da criptografia (CRIPTO), o COMPUSEC está relacionado com a segurança dos computadores, das máquinas e programas que processam a informação (*Hardware, Software e Firmware*).

Num ecossistema Ciber há também que considerar as cada vez mais fundamentais Operações em Rede de Computadores (IDN, 2013). Estas operações estão diretamente relacionadas com as atividades que têm lugar no Ciberespaço, como a Exploração de Redes de Computadores que nos permite conhecer e compreender o que está a acontecer neste espaço virtual utilizado como autoestrada de Comunicações para o Comando e Controlo dos Sistemas de Informação, ou outra das principais operações relacionadas com a Defesa das Redes de Computadores que nos permite ter os meios para proteger ativamente os Sistemas de Informação e Comunicações.

A junção da tradicional INFOSEC (COMSEC e COMPUSEC) com as Operações em Rede de Computadores já apresentadas cria o conceito de CIBERSEGURANÇA, um campo de ação essencialmente de responsabilidade civil, onde se destacam as organizações de resposta a incidentes de segurança do tipo *Computer Emergency Response Team* (CERT®) ou *Computer Security Information Response Team* (CSIRT) que protegem a qualidade da informação que reside e circula no ciberespaço e das infraestruturas que providenciam serviços críticos à sociedade, através de serviços de monitorização de potenciais ameaças, identificação de vulnerabilidades e de resposta a incidentes.

[19] Baseado no "Concept for Computer Network Operations in EU-Led Military Operations", (EU, 2009).

Finalmente há que considerar um outro tipo de Operações em Rede, a capacidade de realizar Ataques através de Redes de Computadores, o que pela sua natureza estão restringidas às forças militares, seguindo as orientações políticas do Estado. Estas operações de cariz essencialmente militar no ciberespaço têm por objetivo a disrupção, a negação, a degradação ou mesmo a destruição dos sistemas de informação do inimigo. A junção das três componentes de Operações em Rede apresentadas, com a parte de COMPUSEC da INFOSEC, cria o conceito de CIBERDEFESA.

De modo a desenvolver as capacidades de Cibersegurança, o estado português, seguindo as recomendações da União Europeia onde cada estado membro deve implementar uma capacidade de resposta a incidentes de segurança cibernética (EC, 2013), através do decreto-lei 69/2014 de 9 de maio, decidiu criar o Centro Nacional de Cibersegurança (CNCS). O Centro está na dependência direta da Autoridade Nacional de Segurança com "*a missão de contribuir para que Portugal use o ciberespaço de uma forma segura e as suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades"*.[20]

De igual modo, ao nível da Ciberdefesa, seguindo as recomendações da OTAN, reforçadas na cimeira de Gales (NATO, Wales Summit Declaration, 2014), cada país deve desenvolver uma capacidade própria de defesa das suas redes informáticas, através da prevenção, capacidade de deteção, resiliência e recuperação. O ministro da Defesa Nacional publicou o Despacho n.º 13692/2013[21] com a diretiva para a "Orientação Política para a Ciberdefesa", na qual é definida a estrutura de defesa nacional do ciberespaço, operacionalizada através de um *Centro de Ciberdefesa, na dependência do CEMGFA, "constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas."* Compete ainda a este órgão "*A defesa contra as ameaças cibernéticas deve incluir o reforço da proteção das redes, a monitorização e análise dos padrões de tráfego, a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço".*

Em 2015 o governo de Portugal definiu a estratégia nacional de Segurança do Ciberespaço, onde são apresentados como objetivos estratégicos a promoção de "*uma utilização consciente, livre, segura e eficiente do ciberespaço*", a proteção "*dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos*", o fortalecimento da "*segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais*" e a afirmação do "*ciberespaço como um domínio de desenvolvimento económico e de inovação*". (DR D. d., Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015, 2015)

[20] (DR D. d., Instalação do Centro Nacional Cibersegurança, DR, 1.ª série — N.º 89 — 9 de maio de 2014 , 2014)
[21] (DR D. d., Orientação Política para a Ciberdefesa, DR, 2.ª série — N.º 208 — 28 de outubro de 2013 , 2013)

1.4. Objetivo do trabalho

No âmbito do exposto, observa-se que para garantir uma Capacidade de Cibersegurança é necessário definir um modelo para a edificação de uma Capacidade Resposta a Incidentes de Segurança da Informação no Ciberespaço. Neste trabalho de investigação será proposto um modelo usando a abordagem DOTMLPI-I, uma metodologia desenvolvida pelo departamento de defesa dos Estados Unidos e adotado pela OTAN para a implementação de capacidades operacionais.

Para atingir este objetivo serão analisadas diversas políticas e procedimentos no que se refere aos normativos existentes mais relevantes sobre a segurança da informação, com especial atenção à necessária capacidade de resposta a incidentes de segurança da informação. A metodologia DOTMLPI-I será aplicada à edificação da já referida capacidade, bem como ao modo como a OTAN estruturou a sua capacidade operacional de resposta a incidentes, através da edificação do *NATO Computer Incident Response Capability* (NCIRC). Pretende-se ainda identificar as principais metas a atingir nos diversos domínios DOTMLPI-I, para a operacionalização de uma capacidade de resposta a incidentes de segurança da informação no ciberespaço, através da recolha a opinião de profissionais de referência da área da Cibersegurança, utilizando a metodologia de entrevistas escritas.

Finalmente será proposto um modelo de resposta a incidentes de segurança da informação, com vista à sua utilização pelas equipas técnicas de segurança da Direção Técnica das Tecnologias de Informação e Comunicações da Marinha, como contributo para a criação dos núcleos CIRC setoriais, previstos no plano de edificação de uma Capacidade de Ciberdefesa nas Forças Armadas, de acordo com o já referido Despacho n.º 13692/2013 do Ministro da Defesa Nacional. Pretende-se também que o modelo apresentado possa ser facilmente extrapolado para outros organismos estatais ou empresas, que apresentem uma dimensão e estrutura idênticas à da Marinha.

A futura operacionalização desta capacidade na Marinha, de acordo com o modelo proposto, permitirá a validação do mesmo e a identificação dos pontos suscetíveis de melhoria.

1.5. Estrutura do documento

Este documento está organizado em 5 capítulos. No capítulo 2 são apresentadas normas e metodologias existentes para a resposta de incidentes de segurança que serão analisadas para a elaboração da estrutura do modelo proposto. A identificação dos elementos fundamentais de uma Capacidade Resposta a Incidentes de Segurança da Informação no Ciberespaço numa perspetiva DOTMLPI-I, com base no modelo do NCIRC da OTAN e da opinião de profissionais de referência na área da segurança da informação é descrita no capítulo 3. A apresentação e aplicabilidade do modelo proposto será realizado de acordo com um conjunto de procedimentos de validação descritos no capítulo 4. No capítulo 5 serão apresentadas as conclusões e propostas de trabalho futuro.

2. Normas e Metodologias para resposta a incidentes

Com o objetivo de contribuir para a Segurança da Informação, nomeadamente no esforço de garantir a qualidade da informação através das premissas confidencialidade, integridade, autenticidade e disponibilidade, em sistemas cada vez mais abertos e complexos, têm surgido vários normativos recomendando as melhores práticas, especialmente dedicados aos procedimentos e às políticas a adotar ao nível das tecnologias de informação e comunicação. As normas existentes são muito abrangentes e acompanham em detalhe todos os processos nas várias fases do desenho da arquitetura de um Sistema de Informação. Considerando o âmbito deste trabalho, será analisado o contributo de algumas normas mais relevantes, no capítulo específico da gestão de incidentes. Começaremos por abordar a normas da série 27000 da ISO/TEC, mais concretamente a ISO 27002 e a ISO 27035. Também será analisada a *framework Information Technology infrastructure Library* (ITIL), mais orientada para a gestão dos serviços, mas que também apresenta uma abordagem para a gestão de incidentes. Os Estados Unidos e a Europa possuem organizações que produzem normativos relativos à Segurança da Informação, assim, será analisado o documento SP 800-61 do *National Institute of Standards and Technology* (NIST) dos EUA, um guia para a gestão de incidentes de segurança de computadores e também um guia de boas práticas para a Gestão de Incidentes, da *European Union Agency for Network and Information Security* (ENISA).

2.1 Norma ISO/IEC 27002

A norma ISO 27002[22] tem por objetivo estabelecer "diretrizes e princípios gerais para iniciar, implementar e melhorar a gestão de segurança da informação numa organização" (ISO/IEC, 2005) através da implementação de controlos, seguindo a orientação da norma ISO 27001[23].

A norma ISO 27002 está estruturada em 11 secções que se dividem em 39 categorias principais de segurança. Cada categoria principal apresenta objetivos a serem alcançados e os controlos a serem aplicados para que esses objetivos sejam alcançados com sucesso. As categorias abrangem todos os aspetos relacionados com a segurança, aplicáveis aos vários processos específicos do negócio, como por exemplo a Política de Segurança da Informação, a Segurança Física e do Ambiente ou a Gestão da Continuidade do Negócio. Analisamos agora com maior detalhe a secção relacionada com a Gestão de Incidentes de Segurança da Informação.

[22] Publicada em 2005 como evolução da anterior ISO 17799 (27000.org, 2008)

[23] A norma ISO 27001 inicialmente publicada em 2005 em substituição do British Standard 7799-2 apresenta as especificações para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), com vista à sua certificação. A norma permite a orientar da criação do SGSI de acordo com "as necessidades e os objetivos da organização, dos requisitos de segurança e dos processos organizacionais utilizados de acordo com a dimensão e a estrutura da organização" (27000.org, 2008)

No referente à gestão de incidentes de segurança da informação, a norma ISO 27002 releva a importância de se distinguir entre evento[24] e incidente[25]. Um evento poderá nem sempre dar origem a um incidente, mas um incidente tem sempre origem num evento. Os eventos, previstos ou não, podem não comprometer a qualidade da informação (confidencialidade, integridade e disponibilidade) da organização. Os eventos são apenas reportados, mas os incidentes têm de ser geridos, ou seja, existe sempre um momento de análise e decisão para cada evento, de modo a determinar se estamos perante um incidente ou não (Calder & Watkins, 2008). A norma identifica duas categorias principais, o "Relato de fragilidades e eventos de segurança da informação" e a "Gestão de incidentes de segurança da informação e melhorias" para as quais são definidos vários objetivos a alcançar (ver tabela 1).

CATEGORIA	OBJETIVO
Relato de fragilidades e eventos de segurança da informação	Relato de eventos de segurança da informação
	Relato de vulnerabilidades de segurança da informação
Gestão de incidentes de segurança da informação e melhorias	Responsabilidades e procedimentos
	Aprendendo com os incidentes de segurança da informação
	Recolha de evidências

Tabela 1 – Categorias e objetivos da Gestão de Incidentes de acordo com a ISO 27002

Para cada objetivo identificado são especificados os controlos que permitem aferir o grau de sucesso alcançado. Com os diferentes controlos são também disponibilizados guias de implementação para a organização, no entanto, estes devem ser adaptados às suas necessidades específicas de segurança, através da seleção de quais os controlos que melhor se adequam à sua realidade.

Seguindo a organização apresentada na norma, apresenta-se uma análise detalhada dos seus controlos e dos respetivos guias de implementação.

2.1.1 Relato de eventos de segurança da informação

O controlo associado a este objetivo foca-se na necessidade dos eventos de segurança serem reportados através dos canais definidos para o efeito, tão depressa quanto possível. Como guia de implementação é mencionada a necessidade de estar definido um ponto de contacto, um procedimento formal de notificação e deve ser garantido que todos os colaboradores devem ter conhecimento da sua existência. O procedimento de notificação deve de incluir:

[24] Uma ocorrência num sistema, serviço ou rede indicando uma possível quebra de segurança da informação, política ou falha de controlos, ou uma situação desconhecida que poderá ser significativa em termos de segurança. (NIST N. I., 2013)

[25] Uma ocorrência que coloca em risco a confidencialidade, integridade ou a disponibilidade dum Sistema de Informação ou dos seus processos, armazenamento ou transmissão, ou que constitua uma violação ou ameace vir a violar das políticas de segurança, procedimentos de segurança ou as políticas em vigor. (NIST N. I., 2013)

- Mecanismos apropriados de reposta que garantam o acompanhamento das ações desenvolvidas, até o assunto se encontrar resolvido;
- Um formulário para realizar a notificação do evento de modo a ajudar o colaborador a não se esquecer das ações necessárias;
- Indicação do comportamento esperado perante um evento de segurança;
- Referência para um processo disciplinar formal para os colaboradores, fornecedores ou outros, que cometam violações de segurança.

2.1.2 Relato de vulnerabilidades de segurança

Este controlo refere a necessidade de todos os colaboradores, fornecedores ou outros utilizadores dos serviços e sistemas de informação saberem como registar e relatar, qualquer suspeita ou identificação de uma vulnerabilidade nos serviços ou sistemas. O guia de implementação associado a este controlo aponta para a existência de mecanismos de notificação simples e acessíveis à disposição dos colaboradores, fornecedores ou outros utilizadores. Todas as vulnerabilidades devem ser reportadas o mais rapidamente possível à gestão ou ao fornecedor do serviço e a sua verificação nunca deve ser tentada pelo utilizador, pois a sua verificação por utilizadores não especializados em segurança, pode levar a um aumento da ameaça através da exploração involuntária da vulnerabilidade que se pretende evitar.

2.1.3 Responsabilidades e procedimentos

Este controlo pertencente à categoria de gestão de incidentes de segurança da informação e melhoramentos, vem alertar para a necessidade de serem claramente estabelecidas as responsabilidades da gestão e dos procedimentos, de modo a garantir uma resposta ordenada, rápida e efetiva aos incidentes de segurança da informação. Para garantir o sucesso da implementação deste controlo deve ser utilizada a monitorização de eventos para a descoberta de possíveis incidentes, em adição aos mecanismos de relato. A implementação de uma gestão de incidentes deve sempre considerar o seguinte:

- Devem ser estabelecidos procedimentos que permitam abordar os diferentes tipos de incidentes de segurança da informação;
- Para além dos normais planos de contingência, os procedimentos devem compreender também, a análise e identificação das causas do incidente, a sua contenção, o planeamento e a implementação de medidas corretivas, que impeçam este de voltar a ocorrer. Deve compreender ainda a comunicação com todos os que foram afetados pelo incidente, ou envolvidos na sua recuperação bem como o relatório das ações realizadas para a autoridade competente;

- As provas e evidências devem ser guardadas de modo seguro, quer para análise interna do problema, quer como provas forenses para potenciais denúncias de contrato, processo disciplinar ou mesmo criminal. As provas ou evidências recolhidas, poderão ser utilizadas na negociação de uma compensação por parte dos fornecedores de *software* ou de serviços.
- A recuperação após quebras de segurança e a correção das falhas dos sistemas deve ser cuidadosamente controlada. Os procedimentos devem garantir que apenas o pessoal identificado e autorizado tem acesso aos sistemas em produção, que todas as ações de emergência realizadas estão detalhadamente documentadas, são reportadas à gestão e que a verificação da integridade dos sistemas é confirmada o mais rapidamente possível.

2.1.4 Aprendendo com os incidentes de segurança da informação

O controlo associado a este objetivo refere-se ao facto de ter de existir um mecanismo que permita monitorizar e quantificar os tipos, a quantidade e o impacto associados aos incidentes de segurança da informação registados. Através da monitorização dos incidentes é possível identificar os incidentes de maior impacto, que sejam recorrentes e eventualmente, levar ao desenvolvimento de novos controlos.

2.1.5 Recolha de evidências

Este controlo refere-se à necessidade de uma recolha e preservação correta das evidências para que estas possam ser utilizadas numa eventual ação judicial. Para que as evidências recolhidas tenham valor legal, no âmbito de uma ação em tribunal, a organização tem de garantir que os seus sistemas cumprem com todos os requisitos legais para a recolha e preservação da prova.

2.2 Norma ISO/IEC 27035

A norma ISO/IEC 27035 foi publicada em 2011, substituindo a ISO 18044 de 2004[26], com o título de "Tecnologia de informação – Técnicas de segurança – Gestão de incidentes de segurança da informação". Apresenta-se como um guia para a gestão de incidentes de segurança da informação para organizações de média e grande dimensão, ou para organizações externas que forneçam esse serviço.[27]

[26] (SANS, Cyber Security Awareness Month - Day 24 - A Standard for Information Security Incident Management - ISO 27035, 2012)
[27] (ISO/IEC, ISO 27035 - Information technology - Security techniques - Information security incident management, 2011)

Conforme publicado no site da *International Standard Organization* (ISO)[28], a norma fornece uma aproximação estruturada e planeada para:

- Detetar, reportar e avaliar incidentes de segurança da informação;
- Responder e gerir incidentes de segurança da informação;
- Detetar, avaliar e gerir vulnerabilidades na segurança da informação;
- Melhorar continuamente a gestão dos incidentes de segurança da informação como resultado da gestão dos incidentes da segurança da informação e vulnerabilidades.

A norma disponibiliza as orientações necessárias às organizações que pretendem preencher os requisitos definidos na ISO/IEC 27001 e como um complemento à gestão de incidentes abordada na norma ISO/IEC 27002.

Esta norma define um evento de segurança da informação, como uma ocorrência num sistema, serviço ou rede que indique uma possível falha nos controlos, na política de segurança da informação, ou uma situação até então desconhecida que possa ser relevante para a segurança. É também apresentada a definição de incidente de segurança, como um ou vários eventos de segurança da informação inesperados ou indesejados, que têm uma forte probabilidade de comprometer o negócio da organização ou ameaçar a segurança da informação. Tal como na ISO 27002, é relevado que a ocorrência de um evento de segurança não significa necessariamente que tenha havido uma tentativa bem sucedida de comprometimento, ou que tenha qualquer implicação na confidencialidade, integridade e ou disponibilidade da informação.

A implementação dos controlos por si só, não garante que não subsistam algumas vulnerabilidades que possam comprometer a segurança da informação e como tal a ocorrência de possíveis incidentes de segurança da informação. A norma alerta para potenciais impactos, diretos ou indiretos, no negócio da organização, provocados pelos incidentes de segurança, como tal é necessária uma abordagem estruturada e planeada por parte da organização à sua segurança da informação.

Para atingir o objetivo de implementação de uma efetiva gestão de incidentes de segurança da informação, a norma ISO 27035 apresenta cinco fases que se articulam entre si (ver figura 4):

[28] (ISO/IEC, ISO/IEC 27035:2011(en), 2011)

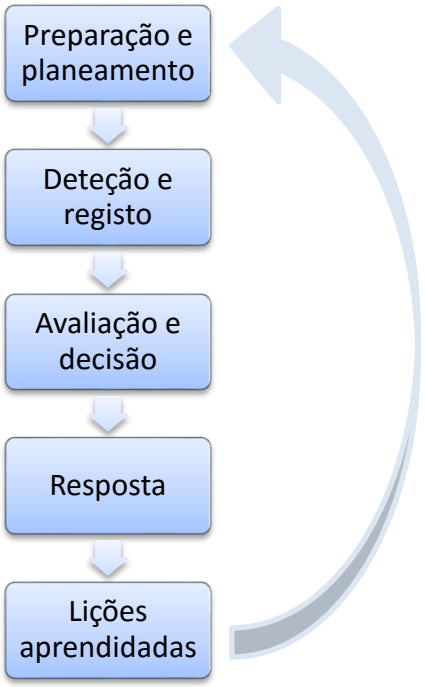

Figura 4 - Fases da gestão de incidentes de segurança da informação

2.2.1 Fase de preparação e planeamento

Para operacionalizar uma efetiva capacidade de gestão de incidentes de segurança da informação, a organização tem realizar uma preparação e um planeamento apropriado, identificando as suas vulnerabilidades, alocando os recursos necessários e esquematizando a sua resposta. A norma aponta um conjunto de atividades a serem completadas para atingir este objetivo.

A primeira atividade é a definição de uma política de gestão de incidentes e o compromisso da gestão de topo da organização com o mesmo. Os colaboradores têm de ser capazes de reconhecer um evento de segurança, saber o que fazer e compreender a mais-valia para a organização da existência de uma política de gestão. Por outro lado, é fundamental que a gestão da organização apoie fortemente a edificação desta capacidade, garantindo os recursos necessários para a manutenção da capacidade de resposta a incidentes de segurança da informação.

Uma atividade que garanta a atualização permanente das políticas de gestão de risco, quer ao nível das redes quer dos serviços, tendo em conta a gestão dos eventos, dos incidentes e das vulnerabilidades da segurança da informação.

É igualmente importante definir um esquema detalhado, que documente o processo de gestão de incidentes de segurança da informação. A norma recomenda a existência de formulários, procedimentos e ferramentas para deteção e relato, com mecanismos de avaliação para apoio à decisão, que aponte as medidas a tomar perante um incidente de segurança da informação, não esquecendo as lições aprendidas resultantes da ocorrência e mitigação do incidente.

A criação de uma equipa de resposta a incidentes de segurança da informação, devidamente formada e treinada, é apresentada como uma das atividades mais importantes. A equipa deve ser organizada e estruturada de acordo com as necessidades operacionais da organização. Pode ser uma equipa com pessoal dedicado, ou uma equipa virtual em que os membros da equipa executam outras funções dentro da organização ou ainda uma solução mista. Por exemplo, pode existir uma equipa permanente dedicada à monitorização, uma equipa técnica de análise avançada, mas que tenha também outras funções atribuídas, sendo ativada sempre que necessário, e outros, como por exemplo os membros de apoio jurídico, que podem ser apenas convocados virtualmente, quando o incidente o justificar.

São incluídas nestas atividades a necessidade de preservar canais de comunicação relacionados com a gestão dos incidentes de segurança da informação, quer internamente, quer com organizações externas relacionadas com este tema.

A norma recomenda o desenvolvimento de programas de treino e de divulgação, não só para a equipa de resposta a incidentes, mas para todos os utilizadores dos sistemas da organização. É importante que todos tenham conhecimento da existência de incidentes de segurança da informação e que a organização possui uma política e procedimentos para o tratamento dos mesmos. Para o sucesso da gestão de incidentes, todos os elementos da organização têm de estar envolvidos.

Finalmente, há que considerar que a gestão de indentes de segurança da informação é um processo dinâmico, sendo por isso necessário assegurar a existência de testes às políticas existentes e a participação da organização em exercícios que permitam testar os processos e a própria equipa de resposta a incidentes, colocando-a em situações de *stress,* em cenários que simulem tão de perto quanto possível as situações reais.

2.2.2 Fase de deteção e registo

A segunda fase de uma operação de gestão de incidentes envolve a sua deteção, a recolha de informação, o relato de eventos de segurança e a deteção de vulnerabilidades, mesmo que estas não tenham ainda sido exploradas, sejam estes descobertos por pessoas ou máquinas. Toda a informação relacionada com um incidente deve ser guardada numa base de dados, operada pela equipa de gestão de incidentes.

Para garantir a deteção, os registos de eventos dos vários equipamentos de segurança (*logs*) como sejam os *firewall*, os IPS[29], os antivírus ou outros, devem ser

[29] *Intrusion Prevention System*

guardados e analisados de modo a integrarem um sistema de acompanhamento dos incidentes[30].

A responsabilidade de notificação de um evento de segurança é pertença de quem o detetou em primeiro lugar. Deste modo, é importante que todos os colaboradores conheçam os procedimentos a adotar quando confrontados com um evento de segurança da informação, de preferência seguindo um guião de como procederem, conhecendo o ponto de contato para comunicarem esse evento. A equipa de resposta a incidentes deve ter alguém escalado para receber e analisar os eventos comunicados ou detetados, decidindo então qual a ação consequente. O registo dos eventos, mesmo que não escalem para incidente, devem ser registados de acordo com um formulário previamente estabelecido de modo a manterem a informação recolhida consistente. Na figura 5 está representado o esquema proposto pela norma ISO 27035 para o fluxo de informação de um evento ou incidente de segurança da informação.

[30] Podem ser utilizados equipamentos de *Security Information and Events Management* (SIEM) que permitem armazenar os eventos registados na diversas plataformas de segurança, correlacioná-los, gerando informação com valor para a equipa de resposta a incidentes da segurança da informação.

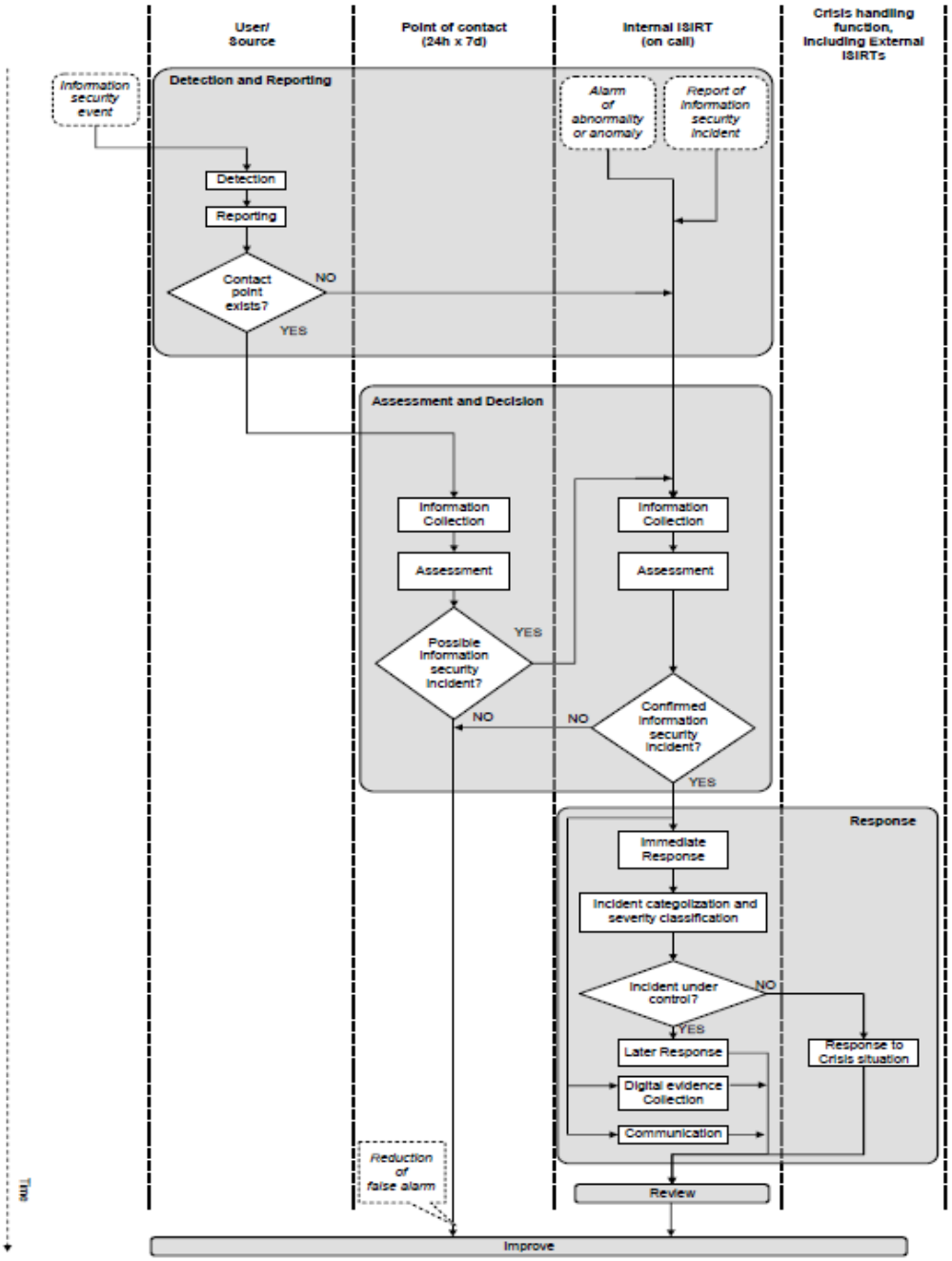

Figura 5 - Fluxo da informação de um incidente de segurança da informação (ISO 27035)

2.2.3 Avaliação e decisão

Nesta fase a norma identifica as atividades referentes à avaliação dos eventos de segurança da informação que permitem escolher os que deverão ser tratados como incidentes.

O membro da equipa de resposta a incidentes de segurança que recebe a notificação do evento, deve avaliar os eventos comunicados de acordo com uma análise de risco feita com base nas vulnerabilidades conhecidas dos sistemas e num conjunto de ações predefinidas. Com base na avaliação feita, o evento deve ser

classificado de acordo com o impacto que este evento pode ter sobre os sistemas e com a forma como pode afetar o modelo de negócio da organização, sendo assim definida qual a prioridade a atribuir à sua resolução ou acompanhamento. Para esta fase a norma indica que todos os eventos devem ser avaliados de acordo com os seguintes elementos:

- Impacto na estrutura física e lógica da organização;
- Os equipamentos, infraestrutura, processos, serviços e aplicações afetados;
- Possíveis efeitos nos serviços nucleares da organização.

Todas as ações relacionadas com o evento e a sua eventual evolução para incidente, devem ser registadas numa plataforma de registo de incidentes que permita o acompanhamento das várias ações executadas e a sua posterior consulta como histórico.

2.2.4 Respostas

Esta fase apresenta as atividades necessárias para responder aos incidentes de acordo com o decidido na fase anterior. Considerando que um incidente se encontra resolvido, a resposta passa pela reposição dos serviços afetados, pela sua documentação e a comunicação às partes envolvidas. No entanto, pode existir a necessidade do incidente ter de ser escalado para um nível técnico superior, ou mesmo para entidades externas à organização. Esta avaliação é feita pela equipa de resposta a incidentes de segurança da informação, devendo sempre ter em atenção durante o processo de resposta a reposição dos sistemas e o registo de todas as ações realizadas, de modo a que a informação não seja comprometida, com vista ao seu valor como prova.

A equipa ao responder ao incidente deve assegurar-se que todos os sistemas estão operacionais e que a vulnerabilidade que lhe deu origem se encontra mitigada, não só no sistema ou equipamento afetado, mas em todos os sistemas idênticos ou que possam ser afetados pela mesma vulnerabilidade. Quando todo o processo estiver concluído, o evento / incidente deve ser formalmente encerrado na plataforma de registo mencionada no ponto anterior.

2.2.5 Lições aprendidas

A última fase refere-se ao que fazer quando o evento / incidente se encontra formalmente encerrado. A primeira coisa a considerar será a avaliação da adequação dos procedimentos estabelecidos para o tratamento do evento / incidente, desde a sua deteção até à reposição dos serviços e mitigação da vulnerabilidade. As conclusões

obtidas a partir desta avaliação, com eventuais melhoramentos a introduzir nos processos e as recomendações para a revisão ou implementação de novos controlos de segurança, devem ser incorporadas na política de segurança da informação da organização e no planeamento das futuras ações de resposta a incidentes.

As lições aprendidas devem ser partilhadas com a comunidade de entidades parceiras da segurança da informação. Esta partilha de informação com outras equipas de resposta a incidentes de segurança de informação, com as quais existam relações de confiança, devem ser feitas de forma regular, pois são importantes para a criação de uma consciência global e de um conhecimento situacional da cibersegurança.

A norma ISO 27035 reforça a ideia que o processo de resposta a incidentes de segurança da informação é um processo iterativo, para o qual a organização deverá estar atenta, procurando introduzir melhoramentos nas suas diversas fases. Para isso os processos devem ser revistos com base nos eventos / incidentes ocorridos e com base nas tendências detetadas.

2.3 A gestão de incidentes no ITIL

A *framework Information Technology infrastructure Library* (ITIL) está orientada para a gestão dos serviços de uma organização numa perspetiva global, sendo muitas vezes utilizada em conjunto com normas de "boas práticas", como por exemplo o normativo ISO 27000 (Arraj, 2010), para serem aplicadas na gestão da infraestrutura, operação e manutenção de serviços de tecnologia da informação (TI). Foi desenvolvido no final dos anos 1980 pela *Central Computer and Telecommunications Agency*, hoje O*ffice for Government Commerce* de Inglaterra.

O ITIL está estruturado em torno do ciclo de vida dos serviços, onde para cada fase são associados processos, ou seja, um conjunto de atividades com vista a alcançar um objetivo específico. Assim, os processos recebem uma ou mais entradas e produzem saídas bem definidas, são mensuráveis e são despoletados por determinados eventos. Os processos podem definir políticas, normas ou guias de resposta (OGC, 2007).

O ciclo de vida dos serviços compreendem cinco fases:

- Estratégia do serviço;
- Desenho do serviço;
- Transição do serviço;
- Operação do serviço;
- Melhoria contínua do serviço.

A gestão de incidentes é um processo que integra a Operação do Serviço, a par da gestão de eventos, da gestão de problemas, gestão de acessos e do preenchimento dos pedidos. Analisaremos agora com maior detalhe a gestão de incidentes.

2.3.1 Gestão de incidentes

Conforme apresentado no manual “ITIL V3 – Service Operation” (OGC, 2007), um incidente é uma interrupção ou quebra de qualidade num serviço de Tecnologia de Informação. Segundo o ITIL, a gestão de incidentes é o processo definido para lidar com todos os incidentes, independentemente da sua natureza ou da sua origem. Os incidentes podem ser comunicados diretamente pelos utilizadores, pela gestão de eventos ou pela equipa técnica que tenha detetado algum incidente, através das ferramentas de gestão de rede ou dos serviços. Nem todos os eventos são incidentes, pois nem todos os eventos são referentes a disrupções de serviço.

O objetivo é a rápida recuperação dos serviços, com o menor impacto possível no negócio. A Gestão de Incidentes no ITIL consiste num conjunto básico de passos (Taruu, 2009):

Deteção – O incidente é conhecido através de qualquer mecanismo, e.g. relato de um utilizador, alerta de um equipamento ou outros;

Registo – Os detalhes do incidente são registados no sistema de gestão de incidentes;

Classificação – O incidente é categorizado de acordo com um critério previamente definido, para facilitar o seu diagnóstico e priorização relativamente a outros incidentes;

Priorização – O impacto e a urgência do incidente são considerados em conjunto, de modo a determinar a sua prioridade relativa aos outros incidentes;

Investigação e diagnóstico inicial – Detalhes adicionais relativos ao incidente são obtidos e comparados com ferramentas como a Base de Dados de erros conhecidos, para a sua resolução;

Escalamento – Se necessário, o incidente pode ser reencaminhado para um outro grupo considerado mais apropriado à sua resolução;

Resolução e recuperação – O serviço é recuperado e é prestado apoio aos utilizadores para retomarem a utilização do serviço;

Encerramento – A resolução com sucesso do incidente é verificada com o utilizador, os detalhes da sua resolução são registados e o incidente é encerrado na plataforma de gestão de incidentes.

Estes passos para a resolução do incidente são sintetizados no *workflow* de gestão de incidentes do ITIL apresentado na figura 6 (OGC, 2007). O *workflow* apresentado mostra que os relatos de incidentes podem ter origem em diversas fontes diferentes. Vimos que todos os incidentes relatados têm de ser identificados, registados, categorizados e priorizados, sendo a sua categorização e atribuição da prioridade de grande importância para a gestão de incidentes de acordo com a infraestrutura afetada pelo incidente. A criticidade dos serviços afetados e o impacto do incidente no negócio

da organização irão ditar a prioridade a atribuir pela gestão de incidentes para a sua resolução.

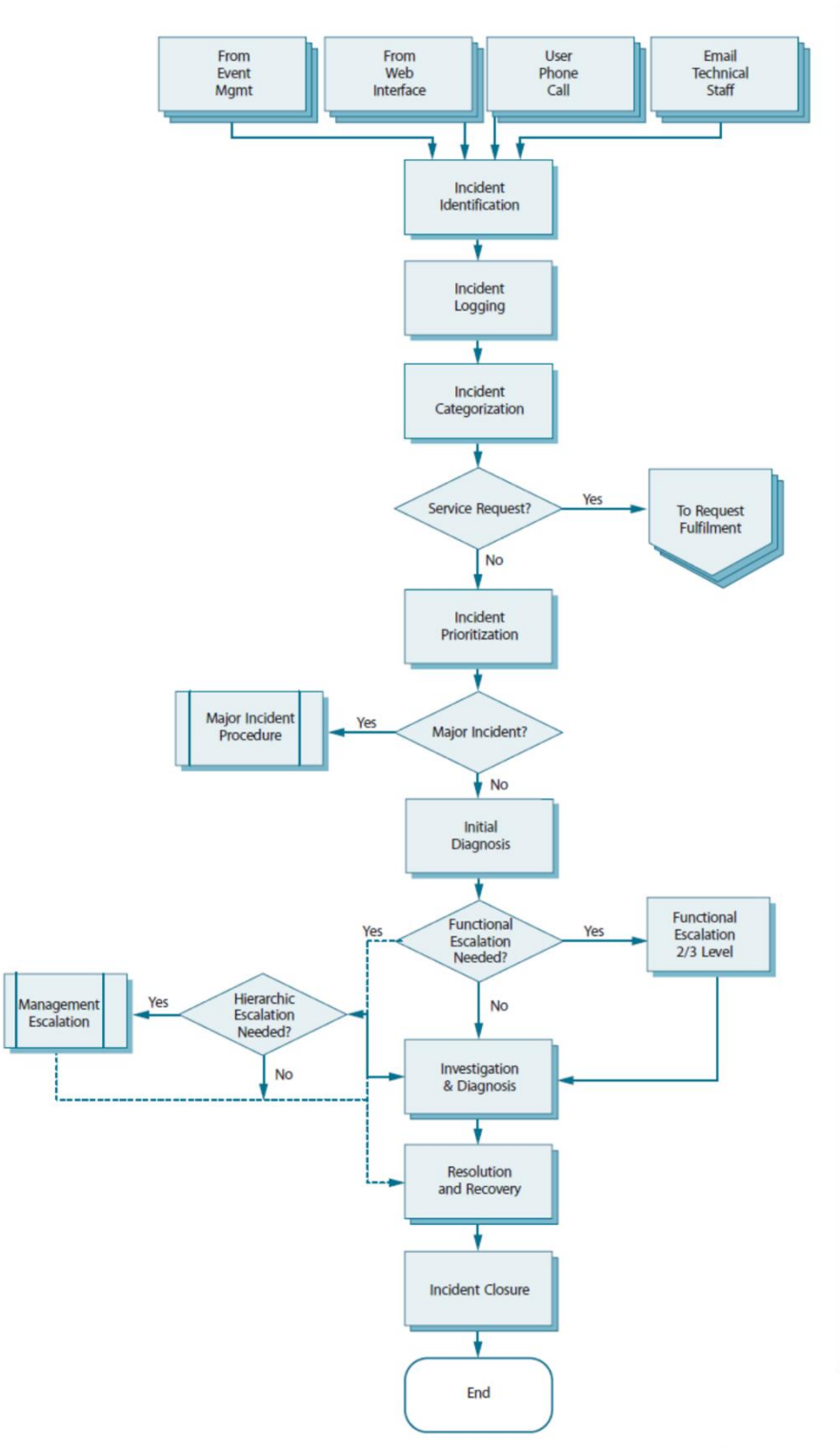

Figura 6 - Workflow da Gestão de Incidentes no ITIL *(OGC, 2007)*

O ITIL prevê a necessidade de determinado tipo de incidentes, que pela sua natureza ou especificidade técnica, tenham de ser escalados, saindo assim da ação

direta do *service desk*[31], mantendo-se no entanto as premissas de investigação, diagnóstico, resolução e encerramento.

O caso específico dos incidentes de segurança da informação são um exemplo desta necessidade de escalar a resolução do incidente para o Departamento Técnico, que deverá, após a sua resolução, fornecer o relatório que permite encerrar o incidente, bem como a disponibilização das evidências recolhidas para efeito de análise forense, ou de eventual processo disciplinar ou jurídico.

O Departamento Técnico deverá ainda colaborar propondo melhoramentos a introduzir nas políticas de segurança ou na operação ou configuração dos sistemas.

No referente à Gestão da Segurança da Informação, o ITIL aborda este tema no âmbito do Desenho do Serviço. Este serviço tem por objetivo a definição das políticas, normas e procedimentos, para garantia dos equipamentos, dos dados e da informação. O ITIL salienta a importância da separação de papéis entre quem define as políticas e os procedimentos, e quem é responsável pela operação dos sistemas, procurando assim evitar situações de conflito de interesse.

2.4 National Institute of Standards and Technology (NIST)

O NIST é uma agência federal norte americana do Departamento do Comércio que tem por missão promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, as normas e a tecnologia de forma a melhorar a segurança económica e a qualidade de vida (NIST, NIST General Information, 2008).

De acordo com a lei federal norte americana publicada em 2002[32] as agências federais devem reportar formalmente todos os incidentes de segurança ao *United States Computer Emergency Readiness Team* (US-CERT).

O NIST publicou o NIST SP 800-61, um guia para a gestão de incidentes de segurança de computadores, com o objetivo de apoiar as organizações e agências federais na mitigação do risco associado aos incidentes de segurança de computadores, disponibilizando orientações sobre como responder a estes incidentes de modo eficiente e efetivo (Cichonki, Millar, Grance, & Scarfone, 2012).

No SP 800-61 o NIST identifica quais as principais ações a realizar para a edificação de uma capacidade de resposta a incidentes:

- Criar um plano e uma política de resposta a incidentes;
- Desenvolver procedimentos para realizar a gestão de incidentes e o seu registo baseados na política de reposta a incidentes;

[31] No ITIL o *service desk* é o único ponto de contacto entre os utilizadores dos sistemas de informação e a gestão de incidentes. Opera quase sempre como proprietário do incidente durante o seu ciclo de vida, independentemente de quem está a trabalhar na sua resolução.

[32] Através da Federal Information Security Management Act (FISMA) de 2012 todas as agências federais norte americanas são obrigadas a criar uma capacidade de resposta a incidentes, devendo obrigatoriamente designar um Ponto de Contacto principal e outro secundário com o US-CERT, reportando todos os incidentes e documentar as ações corretivas realizadas e o impacto desse incidente (US-CERT, 2014).

- Definir as linhas orientadoras para comunicarem com as entidades parceiras sobre os incidentes;
- Escolher um modelo de constituição e operação da equipa de resposta a incidentes;
- Estabelecer relações entre a equipa de resposta a incidentes e outros órgãos internos (e.g. o departamento jurídico) e externos (e.g. forças policiais, órgãos de investigação criminal);
- Selecionar quais os serviços de resposta a incidentes serão disponibilizados;
- Guarnecer e treinar a equipa de reposta a incidentes.

O documento apresenta também um conjunto de recomendações ou "boas-práticas" que deverão ser consideradas pelas organizações, na edificação da capacidade de resposta de incidentes.

Esta capacidade deverá contribuir para prevenção dos problemas que possam evoluir para incidentes, aumentado assim a segurança efetiva das redes, dos sistemas e das aplicações. A documentação dos incidentes e a comunicação com outras entidades relacionadas com o incidente, deve ser feita de modo formal, facilitando a interação e a comunicação, evitando erros de interpretação e comunicando com a entidade certa. É muito importante detetar o incidente o mais cedo possível, criando mecanismos de correlação que permitam a sua automatização tanto quanto possível. Outro aspeto muito relevante está relacionado com o facto de nem todos os incidentes serem iguais no que se refere ao seu impacto na organização, por isso devem de ser definidas linhas orientadoras para a classificação dos incidentes que permitam a sua priorização e devem ser estabelecidos processos que permitam ganhar valor com as lições aprendidas na resolução dos incidentes. Finalmente, durante o tratamento de incidentes de larga-escala, que pela sua complexidade podem não ser facilmente apercebidos pelo colaboradores da organização, é necessário existir um plano de comunicação que consiga alertar todos os colaboradores para o incidente, de modo a todos poderem contribuir com informações que permitam uma ação rápida da equipa de resposta a incidentes. A partilha da informação com outras entidades que também estejam a ser afetadas pelo mesmo incidente permite a tomada de decisões com base em toda a informação disponível.

Para organizar a resposta[33], o NIST começa por apresentar as definições de eventos e incidentes. Um evento é qualquer acontecimento observado num sistema ou rede, como por exemplo os acessos a uma página *web*, o envio de um *email* ou o bloqueio de tráfego numa *firewall*. Por outro lado há que considerar os eventos adversos, ou seja aqueles que cuja ocorrência têm consequências negativas para os sistemas ou para a informação. Excluindo os incidentes relacionados com causas naturais ou falhas de *hardware*, os eventos de consequências negativas são então considerados incidentes. Os incidentes de segurança resultam da violação ou da ameaça (eminência de ocorrência) de violação das políticas de segurança ou das práticas de segurança estabelecidas. O documento apresenta como exemplo de incidentes vários casos (ver tabela 2).

[33] O NIST refere "computer security incident response" que neste contexto iremos considerar como resposta a incidentes de segurança da informação.

Incidente	Descrição
Negação de serviço	Um atacante envia pacotes especialmente adulterados para um servidor ligado em rede (na Intranet ou Internet) de modo a que este bloqueie. Um atacante dirige centenas de máquinas comprometidas para gerarem tráfego de modo a comprometer o normal funcionamento da rede.
Código malicioso	Um *worm* acede aos ficheiros partilhados da organização de modo a infetá-los. Aviso por parte do fabricante de *software* de um novo *vírus* ou *worm* com capacidade de explorar vulnerabilidades existentes na nossa rede.
Acesso não autorizado	Um atacante consegue correr uma ferramenta de exploração de vulnerabilidades conseguindo aceder ao ficheiro de *passwords.* O atacante consegue aceder a informação sensível para a organização.
Uso inadequado	Um utilizador disponibiliza *software* ilegal através de sistemas de partilha de ficheiros. Um utilizador ameaça outro através de *email*.

Tabela 2 – Exemplo de incidentes de segurança (NIST SP 800-61)

O documento do NIST aborda detalhadamente os vários aspetos relacionados com a edificação de uma capacidade de resposta a incidentes de segurança que vão da elaboração das políticas, à organização da capacidade, passando pelo pessoal e os serviços que a equipa de resposta a incidentes pode fornecer à organização. Toda esta informação é sintetizada num conjunto de recomendações, das quais se destaca a necessidade de formalizar a edificação da capacidade de resposta a incidentes, com políticas e procedimentos bem definidos, adaptados à realidade da organização em que se insere. É igualmente importante existirem modelos comunicação e registo de incidentes que facilitem a comunicação interna e a interação com entidades externas. Finalmente a seleção das pessoas certas para os locais certos, com formação e treino adequados, que consigam responder às necessidades operacionais da resposta a incidentes nas suas variadas áreas de intervenção. As áreas são a gestão da capacidade, a deteção e análise ao nível técnico, a capacidade forense ou mesmo o apoio jurídico. O conhecimento do quadro legal aplicável a estas situações é essencial para lidar com possíveis consequências ao nível disciplinar ou para validar a adoção de algumas medidas de monitorização e análise em que as questões legais sejam colocadas em causa[34].

[34] As questões do direito à privacidade e a proteção dos dados pessoais estão previstas na Constituição da República Portuguesa. No seu artigo 35, em especial no seu nº 2, explicita a necessidade de autorização judicial ou do próprio para acesso aos dados pessoais e o seu nº 7 protege ainda os dados pessoais constantes em ficheiros manuais, ou seja arquivos e ficheiros (AR, 2005). O assunto é especialmente enquadrado pela Lei da Proteção de Dados que define a concretização dos direitos, liberdades e garantias que são assegurados pelo artigo 35 da CRP, bem como faz a transposição para a legislação portuguesa das Diretivas europeias nº 95/46/CE, sobre a "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" e ainda a 97/66/CE, "relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações" (DR D. d., Lei da Proteção de Dados Pessoais, 1.ª série-A, n.º 247, de 26 de Outubro de 1998, Lei n.º 67/1998, 1998).

2.4.1 Gestão de Incidentes

O documento editado pelo NIST detalha o processo de gestão de incidentes em 4 fases distintas, a Preparação, a Deteção e Análise, a Contenção, Irradicação e Recuperação e finalmente a Atividade Pós-Incidente. As várias fases, bem como a relação existentes entre elas, são apresentadas na figura 7 no chamado "Ciclo de Vida do Incidente".

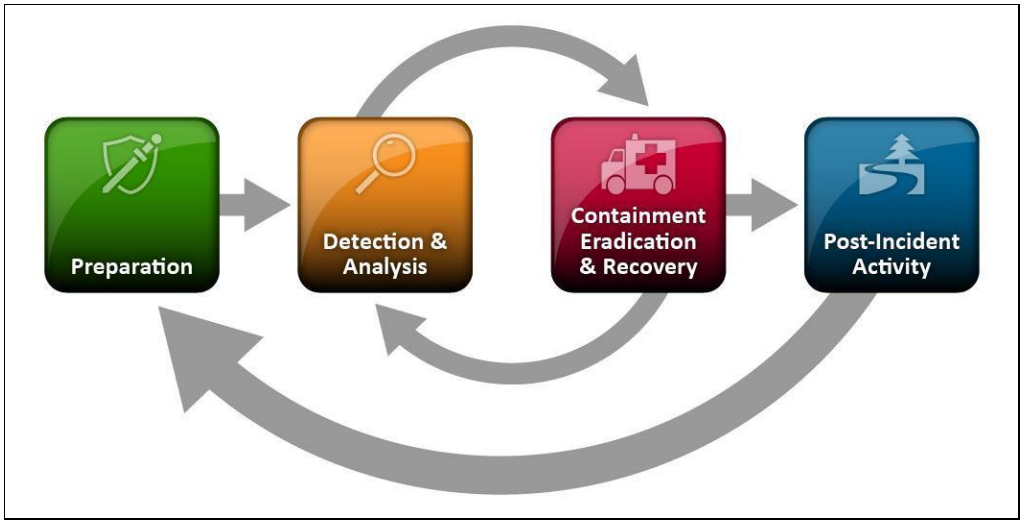

Figura 7 - Ciclo de vida do incidente (Cichonky et al, 2012)

A fase da Preparação tem como objetivos principais a edificação de uma equipa de resposta a incidentes devidamente treinada e equipada[35] e de conseguir limitar o número de incidentes que ocorrem através da seleção dos controlos de segurança adequados a implementar. A equipa de resposta a incidentes deve possuir um *Kit* portátil, com um computador com *software* apropriado instalado e ferramentas que permitam a captura de tráfego de rede e a sua análise forense, a realização de backups e algum equipamento básico de rede, cabos e outro, de modo a que permita uma rápida deslocação a um local para apoio ou para investigação forense[36]. A prevenção de incidentes não está normalmente sobre a dependência direta da equipa de resposta a incidentes, no entanto a sua perceção das ameaças e da sua evolução, permite-lhes a realização de uma análise de risco dinâmica que deve ser considerada na definição dos controlos de segurança implementar na organização.

A Deteção e Análise de incidentes é a fase seguinte. Os tipos de incidentes e o modo como podem atingir a organização são de tal modo variados, que não é

[35] O NIST apresenta informação detalhada sobre *software* específico a utilizar pela equipa de resposta a incidentes e sistemas de apoio como os IDPS (*intrusion detection and prevention systems*), e sistemas de registo (*logging*) centralizado.
[36] A existência destes Kit implica manter a sua constante atualização (sistemas operativos, atualizações dos fabricantes, outras).

possível estabelecer um procedimento para cada tipo de incidente. O NIST propõe a criação de categorias de incidentes e categorizá-los de acordo com o seu modo de transmissão, por exemplo, um vírus que cria uma *backdoor* para obter um acesso ilegítimo deve ser categorizado como "Código malicioso" e não como "Acesso não autorizado". A deteção de incidentes pode assumir particular dificuldade devido ao número de fontes de eventos, que disponibilizam informação sobre potenciais incidentes com diferentes níveis de detalhe e credibilidade, num número particularmente elevado de ocorrências ou eventos e finalmente, porque é necessário muita experiência e um conhecimento técnico muito avançado para uma análise eficiente de toda a informação disponibilizada. O NIST apresenta o conceito de "sinais do incidente" dividindo-o em duas categorias. As "Indicações", como sendo o sinal que um incidente ocorreu ou poderá estar a ocorrer, e os "Indícios" que são o sinal de um incidente que poderá vir a ocorrer. Sempre que um indício seja detetado a organização deverá tomar medidas para prevenir o incidente, no entanto existem muitos ataques que não têm qualquer indício.

A análise do incidente é muitas vezes difícil. Muitos dos sinais recebidos pela equipa de reposta a incidentes correspondem a falsos positivos, a erros humanos de operação ou até a avarias de *hardware*. Muitas vezes as indicações ou os indícios recebidos são ambíguos ou mesmo contraditórios e frequentemente não está disponível toda a informação necessária para categorizar um incidente. Por estas razões assume particular importância a construção de uma equipa experiente, bem formada e devidamente treinada, sob o risco de a deteção e análise dos incidentes ser ineficiente, com os custos de possíveis erros de decisão terem de ser suportados pela organização. Na tabela 3 apresentam-se as recomendações do NIST para uma análise de incidentes mais efetiva.

Recomendação	Descrição
Perfis de rede e sistemas	Criação de perfis de utilização ao nível das máquinas e dos sistemas, nomeadamente ao nível da integridade dos ficheiros críticos. Perfil de utilização da infraestrutura, nomeadamente os valores médios e de pico.
Compreender os comportamentos normais	Análise frequente de registos de desempenho e de operação que permitam detetar desvios e tendências.
Política de Logging	Consolidação dos "*log*" das diversas plataformas numa plataforma centralizadora. Definição de uma política de retenção de "*log*".
Correlação de eventos	Capacidade de correlacionar os "*log*" de diferentes equipamentos (firewall, IDPS, outros) detetando assim indícios de incidentes.
Sincronização de relógios	Utilização do protocolo NTP [37] permite uma efetiva correlação de eventos ocorridos em várias máquinas da organização.

[37] NTP - Network Time Protocol, protocolo que permite gerir a informação de tempo em toda infraestrutura de rede, incluindo máquinas, servidores e ativos de rede, de forma centralizada.

Base de dados conhecimento e informação	Documentação sobre a infraestrutura e vulnerabilidades conhecidas. Informação relativa a *software* malicioso. Informação de domínios maliciosos.

Tabela 3 – Análise de incidentes (recomendações NIST)

Sempre que um incidente é detetado, devem ser prontamente registados todos os elementos disponíveis e a partir daqui, todos os eventos com ele relacionado. A informação recolhida durante a investigação deve ser igualmente armazenada, registada e assinada pelo responsável pela investigação, pois do seguimento correto dos procedimentos, depende a validade da utilização destas informações para utilização em tribunal ou no âmbito de processos disciplinares internos. Deve ser utilizada uma base de dados de registos dos incidentes, que deve conter entre outras, a informação sobre o "estado do incidente", um sumário do incidente, o registo de todas as ações realizadas, o contacto dos intervenientes (utilizadores e gestores), a lista das evidências recolhidas e comentários dos gestores do incidente.

Finalmente, nesta fase há ainda que considerar a classificação do incidente. Esta poderá ser uma das ações mais importantes, pois como os incidentes não são todos iguais e afetam a organização de diferentes formas, é importante fazer uma correta classificação de modo ao incidente ser abordado com a prioridade devida. A priorização a atribuir ao incidente está muito dependente do negócio da organização, ou seja, do impacto que o incidente pode ter do ponto de vista funcional, na segurança da informação. Esta priorização poderá traduzir-se num valor numérico que traduza a severidade e o impacto que o incidente tem para a organização. No caso particular do NIST, que se refere às agências federais americanas, existe uma tabela que permite definir com rigor qual o grau de criticidade do incidente e esta informação deve ser partilhada com o US-CERT.

A fase de Contenção, Irradicação e Recuperação está muito ligada à fase anterior, pois muitas das ações de contenção ou mesmo de irradicação carecem de comprovação na fase de deteção e análise. A contenção é extremamente importante pois após a deteção de um incidente que tenha ocorrido, ou esteja ainda a ocorrer, é necessário responder de modo a limitar ao máximo os seus efeitos. Para isso devem de existir previamente, estratégias e procedimentos de contenção para os diversos tipos de incidentes. Após a contenção do incidente vem obviamente a sua irradicação, no entanto, muitas vezes esta apenas pode ser feita em conjunto com a recuperação, como é frequente nos casos dos incidentes de *malware*, pois a eventual destruição dos ficheiros infetados implica a necessária reposição dos ficheiros afetados, o mesmo se passando perante o compromisso de credenciais de utilizadores, que numa primeira fase poderá passar pela eliminação da conta do utilizador nos sistemas e posteriormente a criação de novas contas. Esta relação é particularmente importante quando os sistemas são afetados ao nível dos seus sistemas operativos. A irradicação

passa muitas vezes por se fazer uma nova instalação do sistema, recuperando no entanto as informações de customização anteriormente existentes.

A Atividade Pós-Incidente desempenha um importante papel no registo das "lições aprendidas" e da identificação das oportunidades de melhoria das políticas, dos controlos e dos procedimentos. Após o encerramento de um incidente importante, toda a equipa deve ser reunida e o processo completo deve ser analisado de modo a averiguar o que aconteceu, como aconteceu e porque aconteceu. Importa também verificar se todos os procedimentos foram seguidos e se foram respeitados os processos de comunicação, retirando daqui valor para que a organização esteja melhor preparada numa próxima ocorrência. Na ausência de incidentes importantes, a equipa deve reunir-se periodicamente e analisar o conjunto de vários incidentes, sempre com o objetivo de identificar melhorias e propô-las para que sejam incorporadas na fase de preparação. No final deve ser elaborado um relatório do incidente com toda a informação sobre o mesmo e com as conclusões resultantes da reunião da equipa e com as sugestões de melhoria. A informação recolhida nesta fase irá contribuir para uma nova análise de risco, para avaliar o desempenho da equipa de resposta a incidentes e auditar a capacidade de resposta a incidentes da organização.

2.5 Guia de boas práticas para a gestão de incidentes da ENISA

A ENISA, como agência europeia para a segurança da informação e redes, apoia os estados membros da União Europeia e as agências europeias, funcionando como um Centro de Excelência que produz avisos e recomendações para os assuntos relativos à segurança da informação e das redes, nomeadamente das infraestruturas críticas europeias (ENISA, Threat Landscape - Responding to the Evolving Threat Environment, 2012). Em 2010 a ENISA publicou um guia para apoio à constituição de um serviço tratamento de incidentes, considerando-o como o núcleo da capacidade de gestão de incidentes (ENISA, Good Pratice Guide For Incident Management, 2010).

Neste guia de boas práticas, a ENISA apresenta a Gestão de Incidentes como um conjunto de serviços mais alargados de segurança a providenciar à organização, como sejam a capacidade de tratamento de incidentes, a análise e mitigação de vulnerabilidades, comunicados e alertas de segurança, entre outros serviços de gestão de incidentes. A figura 8 apresenta a visão da ENISA sobre o serviço de resposta a incidentes, dentro de uma capacidade de gestão dos mesmos. Nela estão representadas as quatro fases principais do tratamento de um incidente, a Deteção, a Triagem, a Análise e a Resposta ao Incidente.

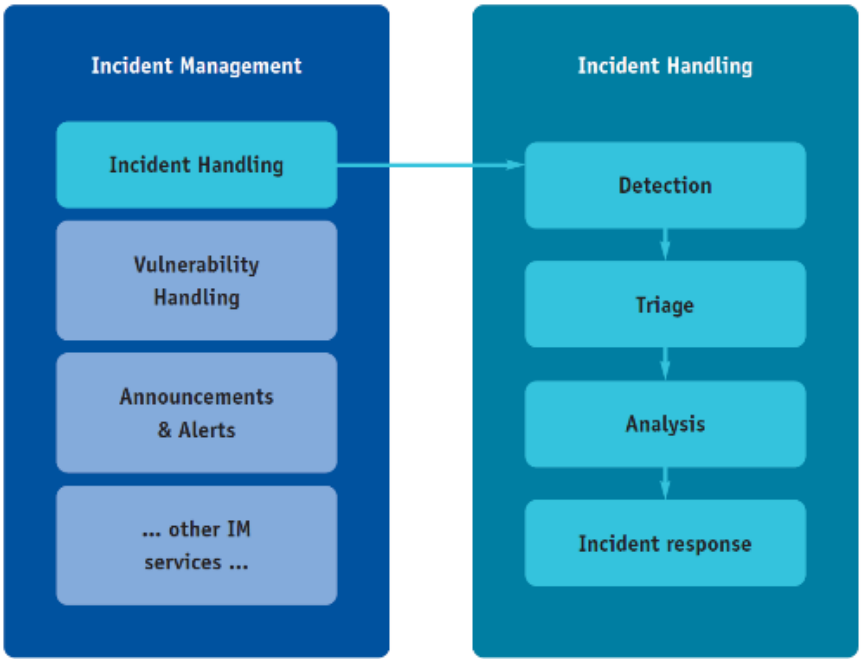

Figura 8 - Gestão de Incidentes e tratamentos de Incidentes (ENISA, 2010)

Para o desempenho das várias fases do tratamento do incidentes, a organização da gestão de incidentes tem obrigatoriamente de prever a existência de uma equipa com pessoal técnico preparado para desempenhar essas funções. A ENISA identifica como funções obrigatórias a existência de um *Duty Officer* responsável pela receção de todos os pedidos ou relatos de incidentes, pela sua introdução no sistema e garantir que todos os incidentes têm um dono. Terá também de existir um *Triage Officer* que irá receber o incidente, fazer a sua triagem e decidir se irá ser endereçado à equipa de resposta a incidentes e a que *Incident Handler* o atribuir. Este papel implica já um conhecimento maior sobre a organização e estar sempre atualizado sobre as ameaças e os seus vetores de ataque. Dependendo do tamanho da Organização, estas duas funções poderão ser desempenhadas pela mesma pessoa. O *Incident Handler* é quem efetivamente atua sobre os incidentes, analisa os dados e executa as ações necessárias à sua resolução. Deve manter uma comunicação estreita com o *Incident Manager*, mantendo-o informado das ações desenvolvidas e do seu resultado no âmbito do tratamento do incidente. O *Incident Manager* é o responsável por todas as atividades de tratamento de incidentes e representa a equipa perante a Organização. Também aqui este papel poderá ser desempenhado pelo *Incident Handler* mais experiente da equipa. Existem outras funções relacionadas com o tratamento dos incidentes, mas que não requerem a existência de um membro permanente, podendo ser requerida a sua participação de acordo com a necessidade, são exemplo os elementos de apoio jurídico ou de relações públicas.

2.5.1 Tratamento de incidentes

Sobre o tratamento de incidentes a ENISA propõe um conjunto de fases organizadas de acordo com um *workflow* (ver figura 9) que pode e deve ser ajustado com maior ou menor detalhe às especificidades da organização.

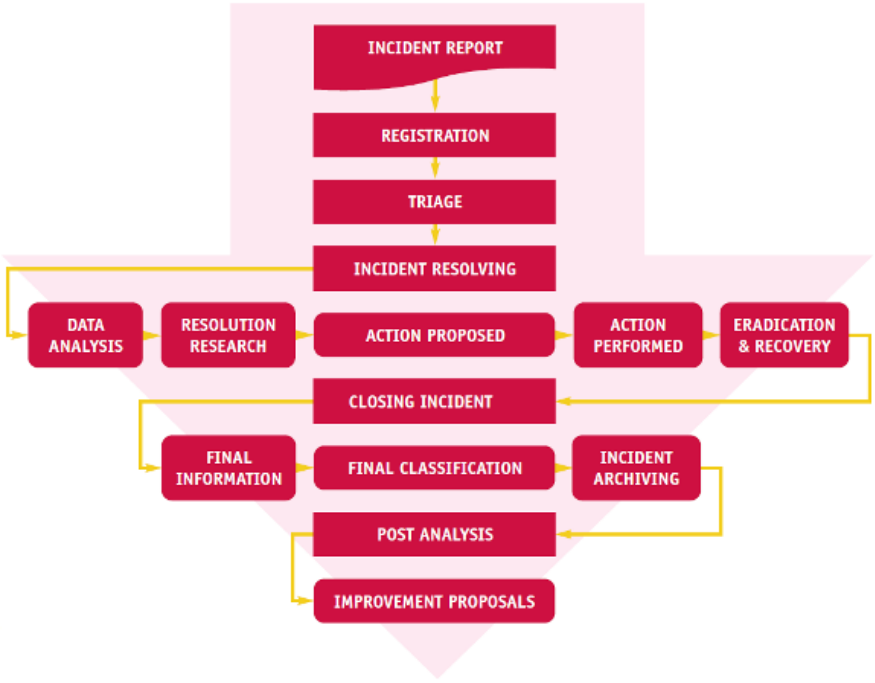

Figura 9 - *Workflow* para tratamento de incidentes (ENISA, 2010)

Fazendo a ligação deste *workflow* com as fases do tratamento de incidentes anteriormente enumeradas, as tarefas de relato de incidente e o seu registo fazem parte da fase de Deteção. A equipa de gestão e tratamento de incidentes recebe informações de diferentes origens, estas podem ter origem em mensagens de correio eletrónico, em telefonemas, ou através de formulários eletrónicos disponibilizados para o relato incidentes, a estas fontes que geram ações de natureza reativa, é importante adicionar a monitorização dos sistemas de segurança da organização que permitem uma abordagem preventiva dos incidentes. Todos os incidentes reportados devem ser registados numa plataforma de gestão que permitirá fazer o seguimento do incidente ou eventualmente adicionar o relato a um incidente já existente.

A fase de Triagem está diretamente ligada à necessidade de estabelecer a pertença no tratamento de incidentes e de os encaminhar para a pessoa ou secção apropriadas à sua resolução. Desta forma, a ENISA indica várias questões que devem ser colocadas nesta fase, das quais destacamos:

- Estamos perante um incidente de segurança?
- É referente aos nossos sistemas?
- Qual o seu impacto?

- Quais os danos colaterais?
- Quantas e quais as pessoas necessárias para tratar deste incidente?

A resposta às questões acima apresentadas permitem a execução das tarefas associadas à fase da Triagem, nomeadamente a Verificação, pois nem todos os relatos estão relacionados com incidentes de segurança, ainda assim este deve ser registado e respondido, se possível com uma breve explicação, porque mesmo não sendo considerado um incidente de segurança, aproveita-se a oportunidade para alertar o utilizador para potenciais ameaças. Estando confirmado que estamos perante um incidente, a próxima tarefa é a sua Classificação, mesmo que ainda não exista informação suficiente para uma clara classificação[38]. Segue-se a tarefa da Triagem corresponde à Priorização do incidente de acordo com a sua severidade e o impacto na Organização. Esta tarefa é fundamental pois no caso de existir um número de incidentes que supere a capacidade de resposta da equipa, é muito importante saber quais os que devem ser tratados em primeiro lugar. Finalmente há que atribuir o Incidente à pessoa da equipa mais habilitada para a sua resolução.

A fase de Análise e de Resposta ao Incidente são apresentadas de forma interligada através do Ciclo de Resolução do incidente (ver figura 10). Este ciclo mostra o conjunto de ações necessárias à resolução do incidente, podendo acontecer existirem várias iterações até se atingir o sucesso. O ciclo inicia-se com a Análise de toda a informação recolhida e com a notificação de todos os potenciais afetados pelo incidente, pois nem sempre as partes mais afetadas são as que reportaram o incidente. A análise da informação deve permitir identificar a origem do incidente e divulgar o mesmo a todas as entidades com possíveis ligações ao incidente. A análise da informação disponível pode ser repartida pelos elementos da equipa que tenham maior competência técnica na área específica do incidente, tendo sempre em atenção a carga de trabalho de cada um.

[38] Esta classificação deve basear-se num esquema taxonómico de incidentes aprovado para a Organização.

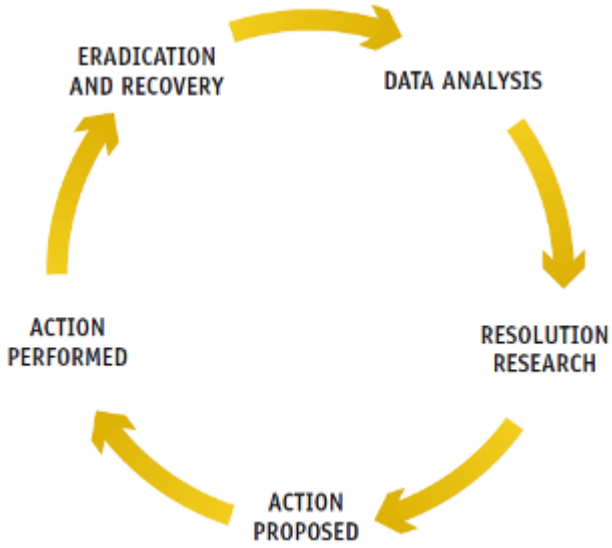

Figura 10 - Ciclo de resolução do Incidente (ENISA, 2010)

Muitas vezes a troca de ideias entre os membros da equipa durante a fase de Análise, leva a que se entre naturalmente na tarefa seguinte, a Procura da Solução. O surgimento de uma possível solução deve ser partilhada com os outros membros da equipa e registada para posterior análise. A definição e a comunicação das Ações Propostas correspondem à próxima tarefa do ciclo. Aqui assume particular importância a comunicação das ações que se pretende venham a ser implementadas por todas as partes envolvidas no incidente, sendo necessário adotar a linguagem ao destinatário da ação. Supostamente as ações propostas foram realizadas, no entanto muitas podem estar fora do nosso controlo e por isso deve-se fazer sempre a verificação das Ações Realizadas. Essa verificação pode ser conseguida através da monitorização dos sistemas, na parte que esteja na nossa dependência, ou através do contacto com os outros participantes externos na resolução do incidente, utilizando-se o correio eletrónico ou outro meio de comunicação. A consequência desejável das ações realizadas é a Irradicação do Problema e a Recuperação. No entanto, se verificarmos que de alguma forma o problema subsiste, mesmo que apenas parcialmente, deve-se fazer nova iteração no ciclo até à total recuperação dos sistemas ou serviços afetados.

A recuperação dos sistemas após a irradicação do problema leva à saída do ciclo de resolução do incidente, conduzindo ao processo de Encerramento do mesmo. O processo passa pela comunicação a todos os envolvidos da resolução do incidente. Uma vez mais a notificação de encerramento deve ser adaptada ao seu destinatário. Para um utilizador normal bastará uma breve descrição do incidente e algumas recomendações para o futuro, no entanto a notificação para outras equipas técnicas que tenham participado na sua resolução, é importante existir uma informação completa, que permita a toda a comunidade evitar a ocorrência de incidentes semelhantes. Esta comunicação irá contribuir para o estabelecimento de importantes relações de confiança entre as equipas. Toda a informação relativa ao incidente deve

ser armazenada de modo seguro (cifra e *backup*) para posterior consulta sempre que necessário, seja para apoio numa nova ocorrência ou para fins legais. De uma maneira geral, esta é uma função que faz parte da ferramenta utilizada para o registo de incidentes.

A ENISA recomenda ainda a realização de Análise *a posteriori* como objetivo de recolher informação relevante que possa contribuir para as lições aprendidas. Para esta análise devem ser apenas considerados os incidentes que mostraram maior complexidade ou que tenham algo de novo no seu processo de ataque. Estas aprendizagens devem ser partilhadas de modo a levarem à eventual revisão das políticas de segurança ou mesmo de processos de operação e de monitorização, contribuindo para a melhoria das condições de segurança dos sistemas e dos serviços. Sendo o serviço de Tratamento de Incidentes fundamentalmente reativo, pode através desta partilha de informação e sugestões de melhorias, contribuir para o melhoramento das políticas de segurança, tendo um efeito preventivo na gestão de incidentes.

2.6 Conclusão

Neste capítulo foi efetuada a análise de vários normativos de "boas práticas" relativas à gestão de incidentes de segurança. Foram selecionados os normativos de referência internacionais como o ISO 27002 e o 27035, a *framework* proposta pela ITIL, bem como a norma norte americana proposta pelo NIST para as agências federais. Foram também apresentadas as recomendações europeias, propostas pela ENISA, para as organizações dos estados membros.

As diferentes normas demonstram *frameworks* de natureza iterativa a que correspondem várias fases no tratamento dos incidentes. Em todas é feito o realce de uma correta preparação para resposta a Incidentes de Segurança. Esta preparação passa pela criação e divulgação de políticas de segurança, pela criação de mecanismos predefinidos de comunicação para o relato de eventos e/ou incidentes de segurança e registo das ações tomadas, sendo igualmente feita referência à necessária preparação e treino da equipa responsável por assegurar a gestão e o tratamento dos incidentes.

Após a deteção de um evento, seja por relato pessoal ou automática através das plataformas de segurança, segue-se uma fase de análise ou triagem, na qual os eventos são classificados e alguns poderão mesmo evoluir para a condição de incidente de segurança. Nesta situação é importante analisar o impacto que a sua ocorrência terá no negócio da organização e atribuir-lhe uma prioridade de tratamento correspondente.

Segue-se a fase de resposta ou de contenção com vista à eliminação das condições provocaram o evento ou o incidente. Esta fase tem como objetivo a total reposição dos serviços de forma segura, sendo para isso necessário proceder também à mitigação das vulnerabilidades que de algum modo permitiram a sua ocorrência.

A tecnologia tem também um papel importante na resposta aos incidentes de segurança. A utilização de plataformas de correlação e análise de eventos, em conjunto com sistema de registo e armazenamento de dados deve ser feito de acordo com os pressupostos legais. Desta forma, os

eventos registados têm valor legal para futuras ações de investigação e podem ser considerados como provas válidas em eventuais processos internos ou de natureza judicial.

A natureza iterativa das *frameworks* leva a que o resultado das ações realizadas seja auditado, através de análise das lições aprendidas. Este facto leva eventualmente a uma alteração das políticas de segurança ou à revisão dos procedimentos estabelecidos. Todas as normas relevam a importância da comunicação com todos os envolvidos, direta ou indiretamente, no incidente. Essa comunicação, quer seja interna, quer seja com entidades externas, é fundamental para aumentar o conhecimento e a consciencialização da organização para as questões da segurança, ajudando a criar relações de confiança entre as partes.

O sucesso da implementação de uma capacidade de resposta a incidentes de segurança da informação está fortemente dependente do compromisso de toda a organização, especialmente das chefias, com as políticas de segurança estabelecidas.

Os conceitos de operacionalização de uma capacidade de resposta a incidentes de segurança da informação anteriormente apresentados, aliados ao processo iterativo das fases do tratamento de incidentes, são estruturantes para o modelo que se pretende apresentar com este trabalho. Relevam-se a estrutura apresentada pela norma ISO 27035 que apresenta 5 fases fundamentais que vão desde o planeamento e preparação das ações, à retroalimentação da informação, baseada nas lições aprendidas e a estrutura organizacional proposta pela ENISA para a gestão de incidentes.

3. Metodologia DOTMLPI-I

O acrónimo DOTMLPI (Doutrina, Organização, Treino, Material, Liderança, Pessoal e Infraestruturas) refere-se aos componentes básicos da edificação de uma capacidade operacional, desenvolvido pelo Departamento da Defesa dos EUA (*Departement of Defense* – DoD). É uma abordagem à implementação de capacidades operacionais, de modo a identificar lacunas na sua operacionalização (ACQuipedia, 2005). A este modelo básico, o DoD viria a adicionar uma outra componente, as Políticas, com o objetivo de adicionar a esta abordagem a procura de procedimentos comuns entre os diversos utilizadores na utilização da nova capacidade. Este novo modelo é conhecido por DOTMLPI-P (DoD, 2013). A OTAN adotou este modelo básico de implementação de novas capacidades fazendo apenas uma alteração, a troca do conceito de Políticas por um outro que lhe é bastante caro, a Interoperabilidade, nascendo assim o acrónimo DOTMLPI-I (NATO, NATO Concept Development and Experimentation (CD&E) Process MCM-0056/2010, 2010).

Antes de abordar a perspetiva militar sobre cada um dos diferentes domínios que compõem esta metodologia DOTMLPI-I e a sua relevância para a edificação de uma capacidade operacional, importa definir este conceito de capacidade. De acordo com a definição da OTAN, uma capacidade operacional é a possibilidade de um comandante militar conseguir executar um conjunto específico de ações, identificando os efeitos necessários para atingir determinado objetivo (NATO, Policy for NATO concept development and experimentation MC 0583, 2009). Desta definição resulta que uma capacidade operacional é complexa e que não se resume a questões de material ou de procedimentos, no fundo é necessária uma abordagem holística como a que permite a DOTMLPI-I, para o sucesso do seu desenvolvimento e implementação.

3.1 DOTMLPI-I uma perspetiva militar

3.1.1 Doutrina

Numa perspetiva militar, a Doutrina aparece ligada ao modo como são conduzidas as operações de combate, sejam as manobras ou as campanhas, ou seja, os princípios fundamentais que permitem a utilização coordenada de uma ou mais forças militares para atingir um objetivo comum. A Doutrina baseia-se os princípios comuns construídos sobre as lições aprendidas durante as operações militares, através de treinos e exercícios. Considerando a sua caraterística imperativa para as Forças militares em campanha, esta está sempre sujeita às políticas comuns acordadas entre as partes, aos tratados e a restrições de natureza legal, devendo ser sempre seguida, exceto se, de forma muito excecional, o comandante em exercício assim o entender.

3.1.2 Organização

A Organização diz respeito ao modo como os indivíduos se constituem como equipas, e estas em unidades operacionais, executando as funções que lhes são determinadas, de forma a contribuírem para o sucesso da missão. Estas unidades

operacionais são suportadas numa estrutura que permite que funcionem de forma coordenada. Esta estrutura tem configurações diversas, de natureza diferenciada e multidisciplinar, conforme se destine às operações propriamente ditas ou a ações de suporte e manutenção. Do desempenho desta estrutura depende em grande parte o sucesso das missões, como tal as ações de Treino assumem particular importância.

3.1.3 Treino

Como descrito no parágrafo anterior, o Treino das equipas é fundamental, sejam estas operacionais ou de suporte às várias estruturas que participam nas operações, sejam unidades individuais, de grupo ou mesmo alianças internacionais. Só o treino permite aos diversos intervenientes num teatro de operações a resposta pronta e capaz às necessidades estratégicas, operacionais e táticas do comando. Uma das formas de executar as ações de treino é através de exercícios que *incorporem os aspetos apropriados do ambiente operacional no cenário de treino, permitindo à audiência de treino a aprendizagem dos conceitos necessários às diversas capacidades, observando a execução do exercício* (DoD, 2013). As lições aprendidas através do treino permitem a revisão ou mesmo o desenvolvimento de novos conceitos com impacto direto no aperfeiçoamento das capacidades operacionais.

3.1.4 Material

O Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais. Esta dimensão abrange desde os equipamentos, à tecnologia, às armas, ou as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão. Os problemas que surgem nesta área podem ter soluções de natureza material, adquirindo o artigo necessário para a sua resolução. Por outro lado também podem ser problemas que não sejam resolúveis através de qualquer aquisição, ou seja, terão de ter uma solução não-material, implicando assim soluções que envolvam alterações nas outras dimensões, como por exemplo na doutrina, na organização ou no treino (E-Maps, 2013).

3.1.5 Liderança

Nesta metodologia a Liderança surge diretamente ligada à Formação, preocupando-se essencialmente com a preparação das chefias para uma abordagem profissional da operação, ou seja ao desenvolvimento da competência profissional para comandar. É fundamental que o líder seja capaz de compreender o objetivo que lhe é apresentado e que conduza a ação para que este seja alcançado com sucesso. Tem de ter a capacidade de dirigir e motivar os membros da equipa, com profissionalismo, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão. Como

refere Cecília Bergamini, *todas as organizações podem contar com bons líderes desde que lhes dispensem o treino adequado e promovam um ambiente favorável onde possam agir com eficácia* (Bergamini, 1994).

3.1.6 Pessoal

No referente ao Pessoal o mais importante é garantir que este possui as qualificações necessárias para o desempenho da missão, quer considerando as necessidades em tempo de paz, quer em tempo de crise. O fator humano e a componente social são determinantes, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e disponibilizarem-lhes a formação adequada. Por outro lado é preciso considerar que para algumas missões, o pessoal pode não ter as competências necessárias, sendo por isso necessário envolver pessoal externo ou parceiros civis, como sejam as empresas do setor tecnológico ou outras, para que se possa cumprir a missão. Quando identificadas lacunas na formação do nosso pessoal, ou o surgimento da necessidade de novas competências relevantes para a missão, deve ser feita a ponderação de alteração do plano de formação previsto para os diferentes papéis que os elementos desempenham no seio da equipa ou a contratualização do serviço a entidades externas. Finalmente há que considerar um quadro de pessoal que garanta a disponibilidade dos recursos humanos necessários quer em tempo de paz quer em tempo de crise.

3.1.7 Infraestruturas

As Infraestruturas são tudo o que se refere com a disponibilização de instalações adequadas à preparação e condução das operações. Também aqui é importante garantir que as Infraestruturas existentes permitem responder de forma satisfatória aos requisitos de manutenção em tempo de paz e aos requisitos operacionais em tempo de crise. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, oficinas, armazéns, centros de dados, estradas, distribuição de energia elétrica e água, entre outras.

3.1.8 Interoperabilidade

A estas sete dimensões básicas do modelo, o DoD dos EUA acrescentou as Políticas, mas a OTAN optou por estabelecer um conceito mais abrangente, a Interoperabilidade. Na verdade a diferença é quase inexistente e podemos mesmo considerar que os objetivos são idênticos. No fundo o que esta dimensão extra do modelo pretende é colocar em destaque a importância de existir uma abordagem comum entre as várias entidades ou equipas que participam nas operações. O estabelecimento desta abordagem comum implica que se utilize um conjunto de

conceitos partilhados entre as partes, que todos entendam como válidos. Isto pode ser conseguido através de políticas que definam procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo. A OTAN define-a como “a capacidade de agir em conjunto de forma coerente, efetiva e eficazmente para atingir os objetivos táticos, operacionais e estratégicos da Aliança” (NATO, AAP-6 NATO Glossary of Terms and Definitions, 2014). De acordo com a missão, existe a necessidade de conduzir as operações num ambiente alargado de parcerias com os nossos aliados por isso a Interoperabilidade assume um papel de destaque na edificação de uma capacidade operacional.

3.2 DOTMLPI-I na perspetiva da Cibersegurança

No ponto anterior foram apresentadas as várias dimensões do modelo DOTMLPI-I, fazendo uma análise básica de cada um dos seus componentes numa vertente de militar. Segue-se uma análise das mesmas dimensões, mas tendo agora por base os conceitos relacionados com a implementação específica de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança, conforme a interpretação resultante da análise de uma importante instituição militar internacional, a NCIRC responsável por esta capacidade na OTAN.

3.2.1 Doutrina

A existência da Doutrina é fundamental na edificação de uma capacidade de Cibersegurança. Através dela são definidos os objetivos e o âmbito em se se inserem as ações a realizar, contextualizando a existência da capacidade em causa, no panorama global das outras instituições e organizações com responsabilidades idênticas e que têm necessariamente de interagir entre si. Dependendo do contexto em que a capacidade se insere, os documentos doutrinários são tipicamente as leis nacionais que regulam as atividades no Ciberespaço, as Estratégias Nacionais para a Cibersegurança, que definem os objetivos do Estado ou das Organizações e o seu âmbito de atuação no Ciberespaço, bem como os documentos doutrinários que definem as políticas de utilização do mesmo e o modo como interagir com os diferentes atores neste domínio. A ausência destas políticas provoca ambiguidades e reduzem a eficácia de uma efetiva capacidade de Cibersegurança. Ao nível nacional, Estratégia Nacional para a Cibersegurança do Ciberespaço apresenta-se como um importante documento doutrinário, não só pela definição dos objetivos estratégicos do país, mas vai mais longe ao apontar de forma inequívoca as orientações para a sua concretização.[39] Apresenta-se ainda como exemplo de documentos doutrinários a Lei

[39]A estratégia nacional de segurança no ciberespaço apresenta como principais eixos de intervenção a "Estrutura de segurança do ciberespaço", o "Combate ao cibercrime", a "Proteção do ciberespaço e das infraestruturas", a "Educação, sensibilização e prevenção", a "Investigação e desenvolvimento" e a "Cooperação" (DR D. d., Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015, 2015)

do Cibercrime,[40] que regula a utilização da informática e criminaliza as atividades ilícitas de natureza cibernética (em complemento a outros crimes já tipificados no Código do Penal), a publicação do Estado Maior General das Forças Armadas PEMGFA/CSI/301 que estabelece a estrutura orgânica, as normas e os procedimentos para garantir a Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas[41] ou a sua equivalente PCA 16 sobre a Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha[42].

O NCIRC tem como principais documentos doutrinários as publicações da OTAN. A publicação AC/322-D/0056 "NATO *Computer Incident Response Capability*" enquadra e regula a edificação de uma capacidade de resposta a incidentes de segurança informática no seio da OTAN, definindo o conceito e os objetivos a alcançar pelo NCIRC, a sua organização, as suas atribuições funcionais, os recursos necessários à sua edificação e um plano de implementação ao longo do tempo. A publicação AC/322-N/0797 "*NATO Computer Incident Response Capability* (NCIRC) *Concept of Operations*" fornece o conceito de operações do NCIRC ou seja a organização, as responsabilidades e os entregáveis desta capacidade.

3.2.2 Organização

A Organização de uma capacidade de Cibersegurança, no seu sentido mais lato, não difere da organização de outras capacidades. Importa definir uma estrutura organizacional que suporte as diferentes atividades que se pretendem implementar e as respetivas relações e dependências hierárquicas e funcionais. Tipicamente existe um nível superior de decisão e coordenação geral, que poderá agregar as atividades que mais se afastam da sua natureza funcional em órgãos de apoio, como por exemplo a assessoria jurídica ou financeira e a gestão do pessoal. No caso de uma capacidade de Cibersegurança é natural que as diferentes valências técnicas e funcionais se organizem em departamentos com objetivos comuns. Como exemplo apresentamos a necessidade de existência de um departamento de operações no ciberespaço que inclua a gestão de incidentes, um departamento para a definição de políticas e normalização, com uma área de auditoria, que deverá ser independente de todas as outras, com a função de validar o cumprimento das normas, um departamento para a gestão da configuração e apoio técnico aos sistemas e às comunicações com um serviço de *helpdesk*.

Considerando a realidade em que o NCIRC se insere, numa organização com 28 países como membros e mais de 120 estruturas civis e militares diferentes[43] que se interligam e comunicam entre si, o NCIRC apresenta uma estrutura que se baseia

[40] (DR D. d., Lei do Cibercrime, Lei nº 109/2009 de 15 de Setembro, 2009)
[41] PEMGFA/CSI/301, de 23 de setembro de 2008
[42] PCA 16, de 16 maio de 2012
[43] A lista completa das estruturas da OTAN pode ser consultada em http://www.nato.int/cps/en/natohq/structure.htm#OA

fortemente na coordenação das várias entidades existentes, com as suas próprias capacidades implementadas, de natureza diversa, com vista a estabelecer-se como uma referência para todas as organizações e agências da aliança, no que se refere à capacidade de responder as incidentes de segurança da informação nas suas redes e na deteção e mitigação de vulnerabilidades (NATO, NCIRC - CONCEPT OF OPERATIONS (AC/322-N/0797), 2002). Para atingir este objetivo o NCIRC está organizado em três camadas principais, hierarquizadas entre si, em que cada uma conta com diversos atores mas com objetivos bem definidos e em que os recursos das várias entidades participantes são utilizados "*o mais possível*" (ver figura 11).

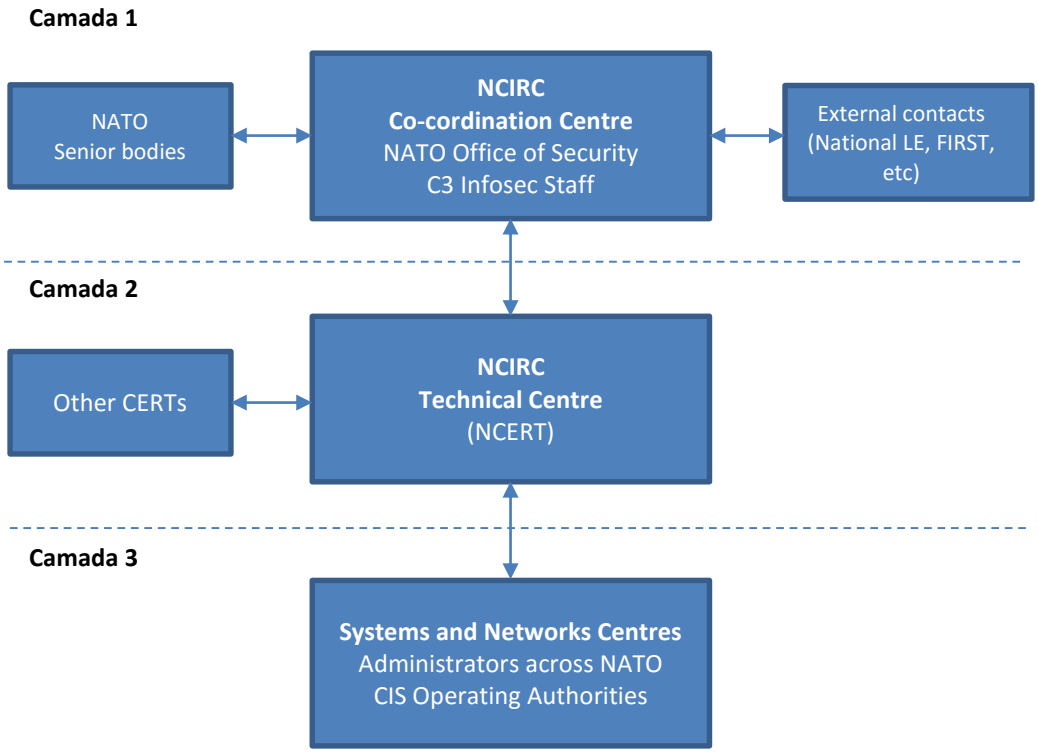

Figura 11 - Estrutura de gestão da NCIRC (baseado em *(NATO, NATO COMPUTER INCIDENT RESPONSE CAPABILITY (AC/322-D/0056), 2002)*)

A camada 1, chamada de "NATO CIRC Co-ordination Centre", é constituída por estruturas de topo da OTAN com responsabilidades na Segurança da Informação e a sua principal responsabilidade é coordenar a resposta aos incidentes, a recuperação da atividade após um incidente ou uma crise, as investigações de segurança e fazer a ligação institucional com outras entidades. As entidades que integram esta camada são responsáveis pelo planeamento anual da atividade do NCIRC, assegurando os recursos financeiros e humanos necessários à normal operação do Centro Técnico de Suporte do NCIRC, designado no referido documento por NCERT e que corresponde à camada 2, que analisaremos posteriormente. Esta camada 1 faz também a ligação com os níveis superiores de decisão da OTAN, nomeadamente através da produção

de relatórios, do estabelecimento do contacto com as entidades externas dos países membros, funcionando como ponto único de contacto para a receção e divulgação de informação sobre as ameaças, assegurando a governação da segurança da informação.

A camada 2 ou NCERT corresponde às atividades técnicas e operacionais do NCIRC para as redes OTAN, nos seus vários níveis de classificação de segurança. O NCERT disponibiliza vários serviços de apoio às várias unidades e agências da OTAN no que se refere à segurança dos sistemas de informação e comunicações ao nível técnico e operacional, nomeadamente na deteção de intrusões e prevenção de *malware,* quer por solicitação das unidades utilizadoras dos sistemas da OTAN quer por determinação Centro de Coordenação. O NCERT tem ainda a responsabilidade de estabelecer canais de comunicação ao nível técnico com as entidades CERT externas, permitindo assim a partilha de informação sobre as ameaças e a divulgação de recomendações de "melhores práticas" a aplicar nos sistemas operados pela OTAN. A comunicação das recomendações para as entidades da camada 3 é feita sob a forma de boletins com informação detalhada. No referente à resposta a incidentes de segurança, o NCERT disponibiliza um serviço de 24x7 para o tratamento dos incidentes e apoio na recuperação dos sistemas, mantendo uma base de dados com informação sobre os incidentes e as vulnerabilidades detetadas, disponibilizando essa informação à camada 1 sob a forma de relatórios que apontam as tendências verificadas ao nível do incidentes de segurança, podendo posteriormente dar origem a recomendações de alterações politicas e procedimentos. A informação sobre os incidentes detetados é divulgada por todas as unidades e agências que operam sistemas de informação e comunicações da OTAN sob a forma de boletins. Esta camada técnica do NCIRC tem ainda como funções a manutenção dos sítios na internet e na intranet classificada da OTAN, disponibilizando informação atualizada sobre vários assuntos relacionados com a segurança, como sejam avisos e informações técnicas, ferramentas de segurança, atualizações do *software* aprovado para uso interno, políticas e boas práticas. O NCERT disponibiliza ainda serviços técnicos avançados, como sejam a análise de vulnerabilidades a sistemas, testes de penetração e análise forense a sistemas comprometidos. Finalmente compete-lhe também uma missão pedagógica, disponibilizando *workshops* e sessões de treino à comunidade de utilizadores dos sistemas de informação e comunicações da OTAN.

A camada 3 corresponde a todas as autoridades (unidades e agências) civis e militares que operam sistemas de informação e comunicações da OTAN. Estas entidades são responsáveis pela administração da segurança e dos sistemas na sua operação diária. A sua responsabilidade primária é realizar a deteção de intrusões, relatar os eventos, incidentes e vulnerabilidades detetados, bem como fazer a prevenção e deteção de *software* malicioso. De acordo com o documento OTAN sobre o conceito de operações do NCIRC (NATO, NCIRC - CONCEPT OF OPERATIONS

(AC/322-N/0797), 2002), estas entidades que operam os sistemas de informação e comunicações da OTAN devem, em estreita colaboração com o NCERT e seguindo as suas orientações doutrinárias e técnicas, garantir a proteção das suas redes e sistemas, nomeadamente no que se refere à deteção de intrusões e de *malware* bem com a sua prevenção. Deste modo o NCERT surge como um órgão de apoio ao qual devem ser reportados todos os eventos de segurança e vulnerabilidades detetadas e seguir as suas recomendações de configuração dos equipamentos de segurança, como por exemplo os equipamentos de *firewall* e de antivírus dos diversos órgãos e agências da OTAN. É ainda da responsabilidade destas unidades a divulgação das recomendações e informações de segurança publicadas pelo NCERT, junto da sua comunidade de utilizadores.

Atendendo à natureza diversa das entidades civis e militares que operam ou utilizam os sistemas da OTAN, o NCIRC prevê o estabelecimento de um *Memorandum de Entendimento* entre o NCERT e estas entidades, definindo claramente os serviços que são da responsabilidade do NCERT e quais os deveres e funções atribuídas às unidades em questão, para além da informação a ser fornecida no âmbito deste acordo.

3.2.3 Treino

O Treino é um domínio essencial do modelo para a manutenção e desenvolvimento de uma capacidade. No caso particular do nosso objeto de estudo, a capacidade de respostas a incidentes de segurança é apresentada com objetivos de treino muito concretos, os quais importa que as equipas e a própria organização atinjam, pois são determinantes para garantir esta capacidade. A capacidade de resposta a incidentes de segurança depende fortemente de equipas com a formação adequada e com processos de atuação perfeitamente interiorizados, pois em algumas situações de elevado risco, a garantia da qualidade da informação depende de uma ação pronta e eficiente. A OTAN organiza anualmente exercícios de natureza cibernética para treino das suas estruturas. Nos exercícios denominados *Cyber Coalition*, a OTAN define como objetivos principais de treino a Capacidade de Decisão, a Coordenação, a Partilha de Informação e o treino das Capacidades Técnicas (NATO, CC14 Training Objectives, 2014). Desta forma assumem-se com principais objetivos de treino a Capacidade de Decisão com base nas informações disponíveis, escolhendo as melhores ações a realizar perante a natureza do incidente, o que devido à grande variedade de ameaças e de fontes de informação disponíveis, requer um treino específico. Outro aspeto que é essencial treinar, é a Coordenação das equipas e dos vários atores que participam no processo de responder a um incidente. É normal o incidente ser detetado, por exemplo numa plataforma de segurança e que os mecanismos de resposta desencadeados com vista à resolução do incidente ou à mitigação da vulnerabilidade, envolvam entidades externas à equipa que está a gerir o incidente, como por exemplo a equipa de administração dos serviços ou comunicações,

sendo fundamental que estas ações sejam bem coordenadas de modo a que atinjam o máximo de eficácia. Na sequência das atividades de coordenação apresentadas, surge como natural o objetivo de treinar a Partilha da Informação. Quando a resposta ao incidente tem de envolver entidades externas é expectável que surjam algumas dificuldades, relacionadas com a utilização de ferramentas e processos distintos, que não permitam uma ação coordenada. Estas dificuldades devem ser detetadas durante as ações de treino, levando à procura e desenvolvimento de processos de comunicação comuns ou pelo menos compatíveis, com vista a uma normalização de procedimentos e de taxonomia. Outro grande objetivo é o treino das Capacidades Técnicas dos vários elementos que compõem as equipas de resposta a incidentes. Para tal é importante que durante o treino sejam simuladas situações tão próximo quanto possível do real, que coloquem os elementos das equipas em situações imprevistas, que os obriguem a explorar completamente as ferramentas que utilizam diariamente, sendo assim possível identificar lacunas na sua formação ou inadequabilidade das ferramentas utilizadas em face da ameaça.

Sendo o NCIRC, especialmente o seu NCERT, o "centro nevrálgico da Aliança na luta contra o cibercrime"[44], o treino das suas capacidades humanas e tecnológicas são fundamentais para o aumento da capacidade de ciberdefesa da OTAN. Desta forma o NCIRC participa regularmente nos exercícios do tipo *Cyber Coalition*[45] que lhe permite treinar os objetivos já anteriormente apresentados, num ambiente de ameaça global em interação com os CIRC militares das nações aliadas e os respetivos CERT nacionais, participando em apoio das respetivas infraestruturas de redes da OTAN, das nações aliadas e parceiras.

3.2.4 Material

Como vimos anteriormente, no modelo DOTMLPI-I o Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais, desde os equipamentos, à tecnologia e às infraestruturas de comunicações. No caso específico da tecnologia utilizada numa capacidade de resposta a incidentes de segurança da informação, iremos considerar quatro categorias distintas, os equipamentos de proteção e monitorização que geram a *informação em bruto*[46], os equipamentos que realizam a agregação e arquivo dessa informação e a correlacionam de modo a gerar informação com mais valor, os equipamentos ou tecnologias que permitem fazer a

[44] (NATO, NATO Rapid Reaction Team to fight cyber attack, 2013), consultado em 14-01-2015

[45] Este é um ciber exercício anual da Aliança que dura 3 dias, testando a sua capacidade de defesa das suas redes contra vários desafios que surgem devido à sua operação no ciberespaço. Este exercício envolve mais de 600 técnicos e especialistas em cibersegurança dos vários países e parceiros da OTAN. Entre outros, este exercício tem o objetivo de testar a rapidez da troca de informação acerca dos ciberincidentes. (NATO, Largest ever NATO cyber defence exercise gets underway, 2014), consultado em 17/01/2015.

[46] Por informação em bruto entendemos a informação tal como é gerada pelos equipamentos de segurança, ou seja, não foi alvo de qualquer tratamento prévio, servindo como exemplo os registos de atividade, de comunicações ou processamento de informação, normalmente designados por *logs*.

gestão da informação sobre os incidentes, e por ultimo, as tecnologias de análise que permitem a investigação do incidente, nomeadamente a investigação forense.

Na primeira categoria temos então os diferentes equipamentos e tecnologias que a organização utiliza, com o objetivo de proteger a informação e as comunicações, adotando estratégias de defesa em profundidade que passam também por estabelecer perímetros de segurança lógicos e físicos, segmentando a infraestrutura da informação em níveis de grau de segurança distintos. Para obter este efeito utilizam-se equipamentos de proteção do tipo *firewall* para controlar e filtrar o acesso aos fluxos de informação entre os diferentes níveis. A comunicação entre níveis é inevitável, bem como a disponibilização e o acesso de serviços de e para o exterior da organização, utilizando-se tecnologias que permitem a autenticação dos utilizadores, que definem diferentes graus de autorização, bem como o registo de toda a atividade realizada. Outra ferramenta que é indispensável na estrutura de segurança da organização, são os equipamentos de inspeção e prevenção do tipo IPS[47] que analisam todo o tráfego dados que circulam na rede, detetando padrões de comportamento potencialmente perigosos, podendo agir preventivamente através do bloqueio automático dessas comunicações. Consideramos ainda nesta categoria as tecnologias de anti *malware* como sejam os programas de antivírus de gestão centralizada ou as plataformas de proteção de correio eletrónico. A utilização destas ferramentas permite ter um conhecimento situacional do ciberespaço da organização, através da análise da informação disponibilizada através dos vários registos de atividade (*logs*) ou dos quadros informativos que disponibilizam.

O conjunto de equipamentos e tecnologias que protegem a informação da organização, abordados no parágrafo anterior, geram eventos de informação em tal quantidade que numa organização de média dimensão (cerca de 8000 utilizadores) pode chegar facilmente aos 1000 eventos por segundo, tornando impossível um tratamento eficaz da informação recebida, que permita realmente saber o que está a acontecer na infraestrutura de informação e comunicações da organização. Para solucionar estes problemas são utilizados os equipamentos da segunda categoria indicada anteriormente. As tecnologias de *Security Information and Events Management* (SIEM) permitem agregar toda a informação gerada nas várias plataformas de segurança, correlacioná-las entre si e com outras fontes de informação externa, como a análise de vulnerabilidades ou informações de inteligência.[48] Assim, os milhares de eventos são transformados em algumas poucas dezenas de potenciais incidentes. Caberá à equipa de resposta a incidentes analisá-los, classificá-los e reagir no caso de estarmos perante um verdadeiro incidente. Os equipamentos que implementam esta tecnologia têm também a capacidade de armazenar os vários

[47] IPS - Intrusion Prevention System

[48] Estas informações de inteligência, conhecidas por Cyberfeeds, são informações recolhidas e divulgadas em tempo quase real sobre eventos de segurança, recolhidos em todo o mundo e pre-processados para as organizações subscritoras destes serviços. (Anubisnetworks, 2015), consultado em 17/1/2015.

registos que recebem, no seu formato original, servindo como fonte de evidências com valor legal, no caso de uma investigação para apuramento de responsabilidades.

A categoria de tecnologias que permitem fazer uma efetiva gestão do incidente está relacionada com a necessidade de existir uma plataforma única que permita seguir o incidente ao longo de todos o seu ciclo de vida, registando todas as ações com este relacionada, desde o relato dos eventos, as ações de triagem realizadas e que levaram à sua escalada para incidente. Nesta plataforma são igualmente registadas as várias ações e iterações efetuadas com vista à resolução do incidente pelos técnicos intervenientes no processo e finalmente as recomendações ou lições aprendidas. Toda esta informação é assim registada numa plataforma associada a uma base de dados, com um interface que permite registar todas as ações relativas à gestão do incidente[49]. Algumas plataformas deste tipo têm também associado um sistema de seguimento das várias ações realizadas, por quem as realizou, disponibilizando ainda um conjunto de ferramentas básicas de apoio à gestão do próprio incidente.[50]

Na última categoria consideramos os equipamentos ou tecnologias utilizados para a análise dos dados e informações disponíveis, com vista à investigação das causas e os efeitos, provocados pelo incidente. Para identificar todos os acontecimentos relacionados com um incidente, é necessário utilizar tecnologias que permitam capturar e analisar pacotes de dados, analisar as configurações base dos sistemas de informação, bem como detetar as alterações introduzidas nos sistemas de ficheiros ou nos registos de configuração dos sistemas operativos, no decorrer do incidente. As plataformas que implementam estas tecnologias têm de estar preparadas para lidar com enormes quantidades de dados, em diversos formatos, e ainda de recolher evidências sem introduzirem qualquer alteração à informação original, para não comprometer a utilização da informação recolhida, no âmbito de uma possível investigação legal.[51]Este material deve estar disponível no local principal de trabalho da equipa de resposta a incidentes, no entanto deve também de existir sob a forma de *Kit* de investigação forense, que seja transportável, para permitir a mobilidade dos técnicos da equipa, mantendo toda a sua operacionalidade ou seja, a capacidade de recolher e investigar evidências.[52]

Devido à sensibilidade desta informação, não existe informação desclassificada disponível sobre o Material utilizado no NCIRC. O documento relativo à fase final de

[49] Devido à potencial importância da informação recolhida, relevamos a necessidade de existirem mecanismos de salvaguarda da informação armazenada, recorrendo a tecnologias de *backup* e a procedimentos de *disaster recovery*, que deverão ser testados periodicamente.

[50] O *Request Tracker for Incident Response* (RTIR) é uma das plataformas mais populares de gestão de incidentes, possuindo um sistema de seguimento das ações realizadas e por quem (*tickting)*, apresentando um *workflow* próprio para apoio à gestão de incidentes (JANET), consultado em 17/01/2015.

[51] O *Forensic ToolKit* (FTK) é uma das plataformas mais completas, incluindo funções muito variadas para a investigação forense, como por exemplo a recolha e análise do conteúdo de memória RAM, suporta a análise de todos os sistemas de ficheiros mais importantes, ferramentas de apoio à desencriptação de informação, cópia integral de discos entre outras (Accessdata, 2015), consultado em 17/01/2015.

[52] Devido à importância destas ferramentas para o sucesso da investigação, consideramos de particular importância mantê-las sempre atualizadas, quer do ponto de vista de segurança (eg, atualizações do fabricante), quer do ponto de vista tecnológico.

operacionalização da Capacidade de Resposta a incidentes, apresenta alguns objetivos de investimento em Material, como a aquisição de uma capacidade central de gestão para o NCERT, o estabelecimento de um canal de comunicações entre o NCERT e o NCIRC-CC, a aquisição de *kits* de reação rápida, a implementação de sensores de segurança para as unidades e agências da OTAN (camada 3) e de um sistema de apoio à decisão para a Ciberdefesa. O sistema deve disponibilizar um conhecimento situacional do ciberespaço da Aliança e um sistema de avaliação e gestão do risco (NATO, NATO Computer Incident Response Capability - FOC, 2011).

3.2.5 Liderança

Na edificação de qualquer capacidade, o fator Liderança apresenta-se sempre como um fator muito importante. No caso da Capacidade de Resposta a Incidentes de Segurança da Informação, existe como fator determinante a abrangência da ação da equipa de resposta, e o impacto das suas ações de forma transversal em toda a organização. Assim, é muito importante que a implementação desta capacidade tenha o apoio inequívoco dos líderes da própria organização. Por outro lado, esta é uma capacidade que está associada a uma forte componente tecnológica, como tal é fundamental a preparação das chefias das equipas para uma abordagem profissional das operações, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão. Nesta perspetiva, o líder da equipa é visto mais como um decisor que tem de possuir um conhecimento holístico da estrutura da organização e dos seus sistemas. A tomada de decisão ocorre muitas vezes em plena ação e desenvolvimento dos acontecimentos, sendo assim importante que o líder esteja preparado para lidar com a gestão de crises no seu ciberespaço organizacional, que conheça os fatores que afetam e irão ser afetados pela sua decisão, de maneira a que o habilite a tomar decisões prontas e fundamentadas. No apoio ao líder podem existir sistemas de apoio à decisão baseados em multicritérios que não serão abordados no âmbito deste trabalho.

Outro ponto que assume especial importância, na gestão da capacidade de resposta a incidentes de segurança, está relacionado com o posicionamento do líder e da sua equipa, na estrutura hierárquica da organização. Devido à abrangência das ações a realizar no âmbito da auditoria aos sistemas e análise de vulnerabilidades, transversal aos vários departamentos, parece-nos particularmente importante assegurar na estrutura da organização, a total separação entre a equipa responsável pela gestão de incidentes e as equipas responsáveis pela administração e configuração dos sistemas de segurança e de suporte aos serviços. Esta separação evita situações de conflito de interesse entre os membros das duas equipas e evita situações de "promiscuidade" técnica, como por exemplo o de um técnico ter de avaliar a

vulnerabilidade de um sistema por si configurado. Finalmente, as ações e as recomendações relativas à segurança da informação, resultantes da análise de vulnerabilidades, da avaliação do risco e das lições aprendidas, deve ter um peso institucional elevado, devendo por isso o líder e a sua equipa estarem posicionados na dependência direta da Direção da organização.

Esta situação está assegurada no NCIRC, pois como vimos anteriormente, a estrutura adotada de três camadas garante que a responsabilidade técnica de responder aos incidentes (camada 2) está separada da responsabilidade de coordenação e de supervisão, a cargo no NCIRC CC (camada 1) e da responsabilidade da implementação das medidas de segurança, a cargo das várias unidades e agências (camada 3).

3.2.6 Pessoal

Numa capacidade de resposta a incidentes de segurança, mesmo existindo todo o material necessário para a sua operacionalização, o Pessoal ou fator humano é determinante, pois tem sempre de existir uma fase muito importante de análise e decisão das ações a seguir. A organização deve disponibilizar os elementos mais capazes para o desempenho das tarefas a realizar, garantindo que estes são possuidores das qualificações técnicas necessárias para o desempenho da missão. Neste sentido é particularmente importante definir os diferentes papeis que cada membro da equipa terá de desempenhar, aprovar o percurso de formação necessário para o desempenho dessas funções e selecionar os elementos. Nas organizações em que existe implementado o conceito de rotatividade de pessoal, é importante garantir a estabilidade dentro das equipas de resposta a incidentes, devido à especificidade das suas ações e da sua formação técnica.

O número e a especialização dos elementos da equipa está obviamente dependente da estrutura definida para a capacidade, que a organização pretende implementar. Uma estrutura exclusivamente interna à organização, com uma configuração centralizada, terá necessidades de pessoal diferentes, de outra de configuração distribuída ou então apoiada por entidades externas.[53]

Tomando como exemplo uma estrutura de resposta a incidentes interna à organização e centralizada, que será a que melhor se adapta à organização fortemente hierarquizada e centralizada da infraestrutura de Tecnologias da Informação e Comunicações (TIC) da Marinha Portuguesa, segundo Killcrece *et al* (2003) a estrutura deverá ser composta por um gestor (garantindo um elemento alternativo para assumir as suas funções), um elemento administrativo e a equipa técnica com formação que

[53] A universidade de Carnegie Mellon apresenta cinco modelos de organização diferentes para as equipas de resposta a incidentes de segurança, o modelo "equipa de segurança", o modelo interno distribuído, o interno centralizado, um modelo interno misto centralizado e distribuído, modelo coordenador (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003). Considerando o objetivo deste trabalho, iremos apenas considerar o modelo interno centralizado.

lhe permita assegurar os serviços a que a equipa tem de responder, em numero suficiente para garantir a operacionalidade desejável de 24x7x365. São ainda apresentados exemplos de outros papéis a serem preenchidos como o de apoio jurídico, o de investigador ou de relações públicas que por não terem caracter permanente não são considerados como responsabilidade direta da equipa.

Killcrece *et al* (2008) identifica como principais fatores para o pessoal, a variedade de competências. As equipas de maior sucesso caracterizam-se por serem dedicadas, inovadoras, flexíveis, analíticas, orientadas para a solução, bons comunicadores e capazes de trabalhar em situações de stress. Killcrece destaca ainda competências técnicas necessárias, ao nível de experiência na administração de redes e de sistemas, experiência em diferentes sistemas operativos, compreensão básica de protocolos de Internet e conhecimento básico sobre os ataques mais comuns a computadores e sobre vulnerabilidades. Na área mais específica da segurança, indica como fatores importantes, a experiência na gestão de incidentes e a capacidade de resolver os problemas.

3.2.7 Infraestruturas

Uma capacidade de resposta a incidentes de segurança da informação não é muito exigente ao nível das Infraestruturas requeridas. Atendendo a que a informação a proteger tem diferentes níveis de segurança, que implicam muitas vezes a segregação física ao nível da própria infraestrutura, é essencial que essa segregação se estenda até ao local onde a equipa de resposta a incidentes monitoriza e analisa os diversos eventos, bem como ao armazenamento da informação relativa aos incidentes de segurança. Assim, nesta dimensão consideramos como fator mais importante, a segurança física das instalações. O edifício onde está operar a equipa de resposta a incidentes, para além da necessária proteção elétrica que permita manter a operar os seus sistemas, mesmo em caso de corte de energia[54], e das condições ambientais, terá também de possuir áreas de segurança para a operação dos sistemas, com os devidos mecanismos de controlo de acessos e de videovigilância.

3.2.8 Interoperabilidade

A Interoperabilidade é fundamental no processo de responder aos incidentes de segurança da informação de modo eficaz e eficiente, de forma a não só resolver o incidente e recuperar a operacionalidade, mas também a mitigação das vulnerabilidades. É um processo complexo que muitas vezes envolve não só a própria organização mas também entidades externas, sejam elas prestadoras de serviços de comunicações, serviços de internet, ou mesmo entidades congéneres. Estas entidades

[54] O edifício deverá apresentar duas linhas principais de energia elétrica, uma associada a sistemas de proteção do tipo U*ninterrupted Power Supply* (UPS), ao qual se associaram todos os sistemas críticos para a operação, e outra associada a um sistema de mecânico de geração de energia.

> externas naturalmente terão os seus processos próprios de operação, com procedimentos e taxonomias diversas das nossas. As ameaças cibernéticas à segurança da informação são globais e na maioria das vezes afetam todas as organizações, independentemente da sua natureza ou área de negócio. O estabelecimento de relações de confiança entre as várias entidades responsáveis por assegurar a resposta a incidentes de segurança, permite a partilha de informação e mesmo de apoio mútuo, na resolução de incidentes de natureza global, permitindo assim um conhecimento situacional do ciberespaço que vai para além do da própria organização. Para que estas partilhas de informação sejam possíveis, é necessário estabelecerem-se não só as já referidas relações de confiança mas também mecanismos que permitam a comunicação clara, com procedimentos e taxonomias comuns.[55]
>
> Para além da relação funcional que o NCIRC possui com as diversas entidades e agências da OTAN na área da segurança da informação, também fomenta estas relações de interoperabilidade com os CIRC militares dos países membros da OTAN e aliados não membros. Existem ainda protocolos de cooperação estabelecidos com a ENISA e outras entidades relevantes para a cibersegurança da OTAN.

A análise que realizámos das diferentes dimensões DOTMLPI-I com base os conceitos relacionados com a implementação de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança e a sua interpretação na aplicação ao conceito NCIRC da OTAN no ponto anterior, permite compreender alguns dos aspetos essenciais à implementação de uma capacidade desta natureza. Da Doutrina é relevada a importância de estarem definidos os princípios legislativos, que irão enquadrar a ação da equipa de resposta a incidentes relativamente aos seus objetivos e o âmbito da sua ação. A Organização é muito importante nomeadamente na articulação e comunicação da capacidade dentro da própria organização. Neste ponto é destacada a estrutura de níveis adotada pelo NCIRC, que permite a separação entre o nível técnico, a coordenação e a comunidade de utilizadores dos sistemas de informação. Do Treino sobressai como mais importante a realização de exercícios internacionais que permitem testar e desenvolver competências ao nível da capacidade de decisão, coordenação, partilha de informação e capacidades técnicas. O Material na capacidade de resposta a incidentes assume relevância no sentido que devem de existir os meios necessários que permitam a monitorização do ciberespaço com mecanismos de deteção e registos de eventos, que eventualmente escalarão para incidentes, assegurando os meios para os acompanhar ao longo do seu ciclo de vida. Da Liderança destaca-se a importância de os níveis superiores de chefia da organização estarem envolvidos em todo o processo de edificação da capacidade, apoiando o seu desenvolvimento,

[55] Como exemplo do esforço de criação de uma verdadeira interoperabilidade a nível nacional, temos o exemplo da Rede Nacional de CSIRT que possui mais de vinte membros efetivos, abrangendo um vasto leque de entidades, que inclui o Centro Nacional de Cibersegurança, as Forças Armadas, vários operadores públicos de telecomunicações, Bancos e instituições universitárias. A Rede assume-se como "fórum de cooperação entre equipas de resposta a incidentes de segurança informática (CSIRT)" tendo acordado entre os seus membros os "termos de referência" que permitirão garantir as condições para uma verdadeira Interoperabilidade. (RCTS, 2015), consultado em 18-1-2015.

motivados pela sua necessidade operacional, dotando-a dos recursos humanos e materiais necessários. Para que esta capacidade seja efetiva, os recursos ao nível do Pessoal devem possuir a formação e o treino que permitam alcançar com sucesso os objetivos elencados na Doutrina, sendo muito importante conseguir garantir a estabilidade das equipas. A Interoperabilidade assume-se como vital na construção da Capacidade de Resposta a Incidentes de Segurança. A complexidade de muitos dos ataques cibernéticos faz com que apenas uma ação concertada de várias entidades permita a sua mitigação. Por outro lado, a partilha de informação e conhecimentos é determinante na construção de um conhecimento situacional do Ciberespaço. A verdadeira Interoperabilidade apenas se concretiza se estiverem considerados dois elementos chave: a existência de relações sólidas de confiança entre os diversos atores que contribuem para a Cibersegurança e os mecanismos de comunicação compatíveis (plataforma de comunicação segura, taxonomia, comum, entre outros).

3.3 Entrevistas a profissionais de referência na área da Cibersegurança

Após a análise das dimensões DOTMLPI-I tendo como base os conceitos relacionados com a implementação de uma capacidade operacional de resposta incidentes e da interpretação da sua aplicação no âmbito do NCIRC da OTAN, pretende-se, no âmbito deste trabalho de investigação, recolher a opinião de profissionais de referência da área da Cibersegurança informação que permita identificar os elementos chave inerentes à construção de uma Capacidade de Resposta a Incidentes de Segurança da Informação que possa ser aplicada no Núcleo de Resposta a Incidentes de Segurança da Informação da Marinha (Núcleo RISI), ou mesmo noutras organizações civis, que procurem edificar esta capacidade.

Para a recolha destas opiniões foi usado o método de entrevista escrita, numa variante de entrevista semidiretiva, que segundo Quivy et al (1998) consiste "*numa série de perguntas-guias, relativamente abertas, a propósito das quais é imperativo receber uma informação por parte do entrevistado*." O guião da entrevista (anexo A) está orientado de modo a obter a opinião dos entrevistados sobre o tema, numa perspetiva de análise DOTMLPI-I. Foram elaboradas oito questões, uma para cada dimensão, em que se pretende a identificação dos fatores que o entrevistado considera fundamentais (críticos) para a operacionalização de uma Capacidade de Resposta a Incidentes de Segurança da Informação. As transcrições exatas das respetivas entrevistas encontram-se anexadas a este texto, de acordo com a ordem com que foram sendo recebidas.

Para análise da informação obtida através das entrevistas, foi utilizada a metodologia de Análise de Conteúdo. Segundo Quivy et al (1998), a metodologia usada " *oferece a possibilidade de tratar de forma metódica informações e testemunhos que apresentam um certo grau de profundidade e de complexidade, como por exemplo, os relatórios de entrevistas pouco diretivas*" o que se enquadra no modelo de entrevista escrita selecionado, aqui segundo a variante de utilização de métodos qualitativos de análise, por serem os mais indicados para um pequeno volume de informação, mas que se apresentam como complexas e pormenorizadas (Quivy & Campenhoudt, 1998). Lawrence Bardin refere ainda que a análise qualitativa permite um procedimento mais intuitivo e maleável relativamente aos métodos quantitativos, sendo especialmente válida na elaboração de deduções específicas sobre um acontecimento ou na utilização variáveis de inferência específica, estabelecendo categorias mais

descriminantes (Bardin, 2003). Estas características da metodologia apresentam-na assim como a mais indicada para a análise da informação obtida através das entrevistas escritas.

A análise da informação de conteúdo organiza-se em 3 fases distintas (Bardin, 2003):

1- A pré-análise que corresponde à fase de organização da informação recolhida e a identificação dos indicadores que serão utilizados na interpretação final;
2- A exploração do material corresponde à aplicação prática dos indicadores identificados na fase anterior à informação recolhida, ou seja, trata-se da codificação ou enumeração de acordo com as regras anteriormente estabelecidas;
3- O tratamento dos resultados obtidos e a sua interpretação permitem estabelecer quadros de resultados, modelos ou diagramas que condensem e coloquem em relevo a informação obtida.

3.3.1 Análise qualitativa do conteúdo das entrevistas

Esta técnica propõe analisar o que é explícito no texto para obtenção de indicadores que permitam fazer inferências. Para o tipo de entrevista em apreço é indicada a modalidade de análise qualitativa (procura-se analisar a presença ou a ausência de uma ou de várias características do texto escrito pelo entrevistado).

Depois de uma primeira leitura de cada entrevista a analisar, codificou-se a informação recolhida de modo a permitir categorizar e salientar trechos da entrevista transcrita, que se passa a apresentar em forma de tabela. Cada tabela está organizada na forma de 3 colunas, Categoria, Unidade de Registo e Unidade de Contexto (Bardin, 2003).

Na coluna Categoria são apresentadas cada uma das 8 dimensões principais que constituíram os temas da entrevista, a saber:

- Doutrina
- Organização
- Treino
- Material
- Liderança
- Pessoal
- Infraestruturas
- Interoperabilidade

Na coluna Unidade de Registo encontram-se palavras retiradas do texto que se tomam por características pertencentes a uma categoria de acordo com a opinião expressa pelos entrevistados. Segundo Bardin (2003), esta "*é a unidade de significação a codificar e corresponde ao segmento de conteúdo a considerar como unidade de base*". Na coluna Unidade de Contexto encontram-se extratos do texto que englobam a Unidade de Registo, contextualizando-a no texto da entrevista, servindo "*de unidade de compreensão para codificar*

a unidade de registo e corresponde ao segmento da mensagem, cujas dimensões são ótimas para que se possa compreender a significação exata da unidade de registo" (Bardin, 2003).

Apresenta-se de seguida uma tabela para cada Categoria (Dimensão) a analisar, seguida de uma análise dos dados recolhidos e das conclusões inferidas das respostas dos entrevistados.

3.3.1.1 Doutrina

Na tabela 4 apresenta-se a análise realizada às entrevistas na dimensão Doutrina:

Categoria	Unidade de Registo	Unidade de Contexto
Doutrina	Objetivo estratégico	"definição clara da missão (objectivos estratégicos) e a sua decomposição em objectivos operacionais"
	Definição de conceitos	"definição de conceitos básicos como ciberdefesa, cibersegurança ou cibercrime para uma melhor definição de missão"
	Comunidade constituinte	"definição do âmbito pessoal (*constituency*)" "a comunidade servida e os *stakeholders* têm que perceber muito bem o papel e os limites de actuação e precisam de se sentir parte de uma máquina maior" "a inclusão na comunidade constituinte de pessoas/entidades sobre as quais não se consegue exercer nenhum tipo de autoridade" "cultura de segurança baseada nos princípios da cooperação (…) dependendo do próprio âmbito de atuação (constituency) (…)" "uma visão que seja acionável e partilhada por todos os intervenientes"
	Comunicação interna	"articulação do CSIRT com outras unidades internas à organização" "forte dependência (…) do departamento jurídico da organização" "deverá moldar uma abordagem de compromissos"
	Comunicação externa	"definidos princípios de colaboração com entidades externas nacionais e internacionais"

		"eficácia das comunicações com o exterior são o indicador que define a reputação (…) no CSIRT" "estabelecimento de redes de confiança"
	Políticas, normas e procedimentos	"políticas de *non-disclosure* que salvaguardem a identidade das vítimas (…) princípios de *need-to-know*" "políticas, normas e procedimentos que (…) dão coerência a toda a capacidade"

Tabela 4 – Análise de conteúdo entrevistas – Doutrina

A análise qualitativa do conteúdo das entrevistas realizadas, no âmbito da dimensão "Doutrina", permitiu identificar alguns aspetos que são considerados essenciais pelos entrevistados para a edificação da capacidade. Conclui-se que é necessária a definição *à priori* do objetivo que se pretende alcançar com a edificação da capacidade e a definição dos conceitos básicos inerentes à própria capacidade, como sejam o conceito de "cibercrime", "ciberdefesa" ou "cibersegurança" para que sejam inequívocos os objetivos da missão. Também foi possível concluir que um dos aspetos mais importantes a considerar é a comunidade de utilizadores para a qual se está a definir a capacidade de resposta a incidentes. A elaboração da Doutrina deve de ter em especial atenção o envolvimento dos *stakeholders* e a aprovação de relações de poder. A capacidade tem de ser construída tendo em consideração a natureza da comunidade alvo (*constituency*), prevendo mecanismos que permitam desenvolver uma cultura de segurança global, integrada com as necessidades de negócio da comunidade e baseada na cooperação com o objetivo de se conseguir o bem comum, a proteção da informação.

Os mecanismos de comunicação interna e externa irão definir em grande parte o sucesso da missão. Internamente é importante a existências de canais simples e diretos de comunicação com os diversos departamentos ou órgãos da organização procurando-se estabelecer com eles relações de compromisso para com o objetivo comum. Da agilidade e eficácia desta comunicação depende uma resposta pronta e atempada aos incidentes detetados. Por outro lado, considerando a natureza global das ameaças e a inevitável interligação de redes com o exterior da organização, a comunicação e o estabelecimento de relações de confiança com entidades congéneres é fundamental para a credibilidade e operacionalidade da capacidade da organização.

As conclusões apresentadas são implementadas doutrinariamente através da definição de princípios, que são traduzidos sobre a forma de políticas ou normas, das quais resultam procedimentos operacionais coerentes com a Doutrina da organização.

3.3.1.2 Organização

Na tabela 5 apresenta-se a análise realizada às entrevistas na dimensão Organização:

Categoria	Unidade de Registo	Unidade de Contexto
Organização	Competências técnicas	"*expertise* para cada uma destas áreas" "as competências e definições de níveis de serviço dentro da equipa deverão ser adequadas às atribuições do CERT" "organizar equipas que reúnam as diferentes competências (…) maximizar a exploração das diferentes competências"
	Enquadramento organizacional	"posicionamento dentro do organigrama da organização de forma a garantir quer a independência, quer a autoridade na coordenação" "o CSIRT esteja colocado fora das áreas funcionais, reportando directamente à direcção ou à administração"
	Coordenação interdepartamental	"devem apoiar ou estar coordenadas com o CSIRT são o departamento jurídico" "o departamento de comunicação/ relações públicas para a gestão de situações mais complicadas do ponto de vista de imagem da organização"

Tabela 5 – Análise de conteúdo entrevistas – Organização

A conclusão que se retira da análise das respostas ao nível da "Organização" incide fundamentalmente em três aspetos. Primeiro devem ser garantidas as competências necessárias que permitam dar resposta ao portfólio de serviços que a capacidade pretende garantir, devendo-se organizar equipas que que reúnam tanto quanto possível todas as diferentes competências identificadas. Em segundo lugar é particularmente relevante o posicionamento orgânico da equipa de resposta a incidentes dentro da organização, devendo estar colocado numa posição diretamente ligada à Direção de modo a estarem garantidas condições de autoridade e independência sobre as áreas funcionais e técnicas administrativas. Finalmente deve estar considerada a articulação com o departamento jurídico para apoio nas situações não previstas na doutrina ou situações de litígio com terceiros e ainda com o departamento de relações públicas para apoio nas situações que de algum modo a imagem da organização esteja colocada em causa.

3.3.1.3 Treino

Na tabela 6 apresenta-se a análise realizada às entrevistas na dimensão Treino:

Categoria	Unidade de Registo	Unidade de Contexto
Treino	Adequação do treino	"identificar as valências técnicas" "desenhar um programa de formação específico"
	Prontidão operacional	"preparação das equipas (…) quando é necessário superar o inesperado" "testar a capacidade técnica a vários níveis"
	Ligação ao real	"ligação dos exercícios ao ciclo de vida da gestão do conhecimento da organização" "identificação das lições (…) aprendidas"

Tabela 6 – Análise de conteúdo entrevistas – Treino

O "Treino" assume-se como uma componente essencial de uma capacidade de resposta a incidentes. Um dos aspetos mais importantes mencionado pelos especialistas está diretamente relacionado com a adequação do treino à realidade operacional em questão. Os programas de treino devem ter em consideração não só as valências técnicas existentes nas equipas, mas também estarem orientados para o treino e teste de condições tão próximas quanto possíveis do real da ação diária da organização. As ações de treino devem ser desenvolvidas de modo a poder testar e treinar os procedimentos e a capacidade técnica de resposta nos diversos níveis de atuação das equipas, quer na sua ação interna, quer na sua ação interdepartamental ou mesmo na sua relação com entidades externas à própria organização. Qualquer ação de treino na verdade só terá efetivamente valor, se dela forem identificadas as "lições aprendidas", que deverão retroalimentar os processos de decisão de resposta, levando a um desenvolvimento crescente da capacidade operacional.

3.3.1.4 Material

Na tabela 7 apresenta-se a análise realizada às entrevistas na dimensão Material:

Categoria	Unidade de Registo	Unidade de Contexto
Material	Ferramentas de comunicação	"mecanismos de cifra para comunicação quer com a comunidade servida, quer com a comunidade de segurança"

		"meios de comunicação com para receber notificações e interagir com *stackholders*"
	Adequação das ferramentas	"dependendo do portfólio de serviços" "recolha de prova" "análise de tráfego" "análise de artefactos"
	Pressão comercial	"boas soluções *open source*" "primazia (…) de determinada ferramenta, relegando para segundo plano os aspetos arquiteturais"

Tabela 7 – Análise de conteúdo entrevistas – Material

Esta dimensão é a que apresenta à partida, menos opções de risco para a implementação da capacidade, uma vez que junto da comunidade segurança encontram-se desenvolvidas muitas ferramentas de qualidade *open source* sob licença, na maioria dos casos, GPL[56]. O mais relevante será assegurar que as ferramentas se encontram adequadas ao portfólio de serviços. Estes requerem frequentemente uma capacidade de monitorização e análise de tráfego de rede. De acordo com os objetivos definidos, poderão também ser relevantes ferramentas para análise forense de artefactos (eg, discos rígidos de computadores), que cumpram com os preceitos legais de recolha de prova. É igualmente importante assegurar canais seguros de comunicações (cifra) entre os membros da comunidade de segurança, de comunicação com todos os intervenientes institucionais (utilizadores e *stackholders*) bem como mecanismos de divulgação de alertas e registo de incidentes. Outro aspeto mencionado alerta para o risco de a atenção se centrar na ferramenta propriamente dita e detrimento de uma abordagem mais holística de preparação da arquitetura de sistemas e serviços otimizada para a segurança.

3.3.1.5 Liderança

Na tabela 8 apresenta-se a análise realizada às entrevistas na dimensão Liderança:

Categoria	Unidade de Registo	Unidade de Contexto
Liderança	Conhecimento	"bons conhecimentos técnicos para realizar uma boa avaliação da situação"

[56] GPL - General Public License (Licença Pública Geral), a licença para programas da Free Software Foundation (Wikipedia, GPL, 2014), consultado em 18/04/2015.

		“conhecimentos básicos de direito e legislação”
	Capacidade de motivação	“capacidade de gerar confiança dentro e fora da equipa” “tirar o melhor de cada um dos técnicos” “os recursos humanos carecem de motivação (…) resultantes de receio ou pressão”
	Capacidade de decisão	“capaz de gerar confiança dentro e fora da equipa” “que consiga adaptar a sua equipa às crescentes de diferentes exigências (…)” “discernimento para efetuar essa distinção e edificar um mapa de competências”

Tabela 8 – Análise de conteúdo entrevistas – Liderança

As características da dimensão “Liderança” aplicada neste contexto, não difere muito das normalmente atribuídas ao “bom líder”. Da análise das entrevistas ressalta como relevante, o conhecimento alargado das várias áreas de competência relacionadas com a resposta a incidentes que vão desde a componente mais tecnológica, aos princípios basilares do Direito. Sendo esta uma área de intervenção onde frequentemente surgem situações de grande pressão e onde uma ação menos adequada por parte da equipa de resposta pode ter consequências importantes para a organização, é muito relevante que o líder demonstre capacidade de decisão, que consiga gerar confiança e motivação entre os membros da equipa para que estes se sintam confortáveis em agir. O líder deve ter um conhecimento profundo da sua equipa, devendo se capaz de focar a ação dos seus membros no que é realmente importante para a organização, selecionando os elementos mais adequados para responderem aos incidentes de acordo com as suas competências, deixando espaço para que estes possam aprender e especializar-se nas suas áreas de competência.

3.3.1.6 Pessoal

Na tabela 9 apresenta-se a análise realizada às entrevistas na dimensão Pessoal:

Categoria	Unidade de Registo	Unidade de Contexto
Pessoal	Perfil	“identificar as competências (…) humanas, identificar as melhores pessoas”

		“Identificar as caraterísticas únicas necessárias ao bom desempenho de funções” “identificar eventuais vulnerabilidades de personalidade”
	Formação[57]	“desenhar um programa específico para cada um” “o quadro de ameaças (…) está em constante mutação, pelo que o programa de formação deve ser revisto periodicamente”
	Competências	“identificar as competências técnicas” “balanceamento incorreto de determinadas dimensões das competências necessárias”

Tabela 9 – Análise de conteúdo entrevistas – Pessoal

Esta dimensão é identificada como sendo uma das mais críticas em todo o processo de resposta a incidentes, levantando questões como identificação do perfil correto (técnico e humano) para o desempenho das funções, a importância da formação adequada, identificar e gerir as competências necessárias. É igualmente importante manter uma atualização constante, face à natureza dinâmica das ameaças.

No referente ao perfil, os entrevistados identificam como importante a capacidade de comunicação, trabalhar em equipa e de lidar com situações de grande pressão. No processo de recrutamento é importante tentar identificar “vulnerabilidades de personalidade” que possam colocar em risco a segurança da informação, frequentemente de natureza sigilosa.

A existência de uma boa base de formação técnica é igualmente muito relevante, devendo ser identificadas possíveis lacunas nessa formação e estabelecer um programa de formação que permita eliminá-las. Os programas de formação deverão ter um caracter periódico de modo a manter um nível de conhecimento tão atualizado quanto possível.

A identificação das competências técnicas de cada um dos elementos da equipa é um fator determinante na hora de atribuir responsabilidades na resposta a um incidente. Num contexto de trabalho em equipa é necessário estabelecer relações hierárquicas de coordenação, sendo necessário ter em atenção que a uma elevada competência técnica, nem sempre está associada uma capacidade de “comando e controlo”, sendo necessário ter este facto em consideração na formação das equipas para a resposta aos incidentes.

[57] Esta unidade de registo “Formação”, incluída na categoria “Pessoal”, foi largamente abordada na resposta relativa ao “Treino” por isso incluem-se aqui algumas unidades de contexto retiradas dessa resposta.

3.3.1.7 Infraestruturas

Na tabela 10 apresenta-se a análise realizada às entrevistas na dimensão Infraestruturas:

Categoria	Unidade de Registo	Unidade de Contexto
Infraestruturas	Segurança física	"acauteladas as condições de segurança física"
	Segurança lógica	"acauteladas as condições de segurança (…) lógica" "segurança da base de dados de incidentes" "segurança (…) de provas recolhidas para efeito de admissibilidade em tribunal"

Tabela 10 – Análise de conteúdo entrevistas – Infraestruturas

Esta dimensão parece ser a que traz menos preocupações aos entrevistados. Na realidade neste campo não são exigidas condições muito especiais que não sejam requeridas noutros serviços que manipulam e armazenam informação sensível. Deste modo será importante garantir a segurança física, nomeadamente ao nível do controlo de acessos e a segurança lógica dos sistemas de informação, sendo talvez o mais crítico, conseguir garantir a integridade e a disponibilidade da base de dados de registo de incidentes.

3.3.1.8 Interoperabilidade

Na tabela 11 apresenta-se a análise realizada às entrevistas na dimensão Interoperabilidade:

Categoria	Unidade de Registo	Unidade de Contexto
Interoperabilidade	Comunicação	"a resposta a incidentes só se faz coordenando com outras entidades" "capacidade de "*intelligence*" que dê algum nível de "*early warning*"
	Confiança	"canais de confiança ágeis estabelecidos com todo o tipo de parceiros" "fomentem a confiança e a obtenção de resultados atempados" "confiança/reputação numa equipa de CSIRT são fundamentais para a partilha de informação"

	Processos	"STIX (…) standard importante se precisarmos de criar mecanismos automáticos de tratamento de informação partilhada" "standard (…) IODEF para partilha de informação sobre incidentes" "definir que tipo de atuação temos relativamente às situações mais comuns e partilhar" "normalização de procedimentos, modelos de dados, informação estruturada"

Tabela 11 – Análise de conteúdo entrevistas – Interoperabilidade

A "Interoperabilidade" é um elemento crucial numa capacidade efetiva de resposta a incidentes. Considerando a variedade e a diversidade de ameaças, às quais se juntam múltiplos vetores de ataque uma capacidade de resposta a incidentes só é possível se for feita de modo cooperativo.

A criação de relações de confiança entre a comunidade de segurança e o estabelecimento de processos de comunicação, ágeis e compatíveis, são os principais desafios que se colocam ao estabelecimento de condições de interoperabilidade. Neste sentido tem sido feito um esforço de se criarem procedimentos, que sejam aceites como *standard* pela comunidade, permitindo a troca de informação de modo seguro, ao mesmo tempo que se tentam definir as ferramentas que permitam o processamento "eficaz e eficiente" da informação, de modo automatizado, facilitando assim os mecanismos de interoperabilidade.

A interoperabilidade entre os diversos atores (privados, públicos, nacionais e internacionais) permite a construção de uma rede virtual de informação, disponibilizando uma capacidade de aviso antecipado, que funciona como uma ferramenta fundamental na proteção contra ataques de larga escala.

3.3.2 Conclusão

Como se pode constatar da análise das respostas obtidas aos especialistas em segurança entrevistados, uma capacidade de resposta a incidentes de segurança da informação é muito mais do que um simples juntar de meios, sejam eles tecnológicos, informacionais ou humanos. Como demonstram as opiniões expressas, essa capacidade resulta da combinação das várias dimensões do modelo DOTMLPI-I, que em graus de relevância distintos entre si, contribuem para a sua edificação, conforme representado na figura 12.

Figura 12 - Modelo DOTMLPI-I e a Capacidade de Gestão de Incidentes

Apresenta-se de seguida uma reflexão sobre as conclusões retiradas a partir das respostas dos especialistas de segurança, tendo como objetivo enunciar os fatores críticos que se pretendem incorporar no modelo de resposta a incidentes a apresentar no próximo capítulo deste trabalho.

O resultado das entrevistas permitem-nos identificar como um dos fatores mais críticos a Doutrina. Esta deve ser clara na definição do objetivo estratégico que se pretende alcançar. Quais as normas, princípios e procedimentos a adotar. É também de elevada importância a identificação inequívoca da comunidade alvo da capacidade e quais os serviços que irão ser prestados a essa comunidade. Finalmente, a definição de uma política de comunicação interna e externa e a definição dos conceitos basilares de segurança para a organização.

Também a Organização foi identificada como uma das dimensões mais críticas para o sucesso da implementação desta capacidade, nomeadamente foram colocados em destaque, fatores como as competências técnicas, atendendo à especificidade das várias áreas de atuação e de prestação de serviços, no âmbito da operação da capacidade de resposta a incidentes de segurança da informação. O enquadramento organizacional é também um fator crítico, pois a organização deve assegurar a total independência da capacidade de análise de vulnerabilidades, deteção e resposta a incidentes, dos departamentos técnicos responsáveis pela administração e gestão da configuração dos sistemas, incluindo das plataformas de segurança. Dependendo da dimensão da estrutura responsável pela capacidade, alguns serviços de apoio específicos poderão não ser residentes na própria capacidade, podendo ser prestados por outros departamentos da instituição, nomeadamente ao nível do apoio jurídico, de grande relevância quer no apoio a ações de natureza litigiosa com colaboradores ou outras organizações, quer colaborando na elaboração de normas e políticas ao nível da sua validação jurídica. Outro serviço que poderá não ser interno a esta capacidade é o de Relações Públicas,

que pela sua especificidade poderá ser assegurado com vantagem pela própria organização, desta forma a coordenação interdepartamental assume grande relevância.

As dimensões de Treino e Pessoal surgem como críticas e fortemente relacionadas entre si. É extraordinariamente importante identificar as Pessoas que tenham um perfil adequado ou seja, capazes de agir corretamente sobre pressão, com boa capacidade de trabalhar de forma cooperativa e facilidade de comunicação. A organização deve identificar claramente as competências que são necessárias, em virtude dos objetivos a que se propõe alcançar, proporcionando condições de aprendizagem e consolidação de conhecimentos, recorrendo as ações de formação que poderão ser de natureza interna ou externa. Mesmo tendo as pessoas certas e com a formação adequada, para que exista uma verdadeira capacidade operacional é necessário garantir o seu treino de modo continuado. A natureza dinâmica das ameaças e a multiplicidade de fatores que podem afetar a segurança da informação, exigem equipas treinadas, desejavelmente em ambientes que sigam tão próximo quanto possível os cenários reais que podem afetar a organização. A existência de exercícios de treino num ambiente multiorganizacional, em complemento a outros de natureza exclusivamente interna, são muito importantes para o estabelecimento de importantes relações de confiança e teste de canais de comunicação ao nível horizontal entre CSIRT.

Ao nível do Material importa garantir a existências de ferramentas adequadas tendo de existir a preocupação de a atenção ser mais holística, ao nível da arquitetura dos sistemas e dos serviços, e vez de se centrar na ferramenta propriamente dita. Estas ferramentas devem permitir uma capacidade de monitorização, análise de tráfego de rede bem como a análise forense de artefactos cumprindo com os preceitos legais de recolha de prova.

Numa capacidade de resposta a incidentes de segurança da informação é natural que surjam muitas vezes situações de natureza complexa e de grande pressão psicológica. Neste contexto, também a Liderança foi considerada com um fator de natureza crítica. A Liderança pode neste caso ser considerada a dois níveis diferentes. Por um lado temos a Liderança ao nível da própria organização, que se deve constituir como um dos principais apoiantes da atuação das equipas de resposta a incidentes, dando assim uma maior relevância interna à capacidade de resposta a incidentes, funcionando como um elemento facilitador na implementação de políticas e procedimentos, nem sempre populares ou bem compreendidos pela comunidade constituinte. Noutra perspetiva há que considerar o papel da Liderança ao nível operacional, coordenando diretamente as equipas que asseguram esta capacidade. Neste contexto, o Líder deve possuir uma sólida formação na área da segurança e ser reconhecido pela sua competência técnica. Para além destas qualidades técnicas, deve igualmente ter uma elevada capacidade de decisão, pois mais uma vez se releva a possibilidade de surgirem situações de grande criticidade para a segurança da informação, onde o tempo de resposta e a decisão atempada podem fazer toda a diferença no grau de comprometimento dos sistemas e da informação. Por fim, é também importante que o Líder tenha a capacidade de se aperceber do “estado de espírito” das suas equipas e ter capacidade de os motivar, mesmo perante situações de grande *stress* ou de resultados menos positivos.

Ao nível das Infraestruturas o mais relevante será garantir que estas apresentem as necessárias condições de segurança (físicas, elétricas, ambientais) que assegurem a integridade e a disponibilidade de informação, nomeadamente a contida na sua base de dados de registo de incidentes.

A última dimensão analisada foi a da Interoperabilidade e também ela se apresenta como crítica para a edificação e operacionalização de uma capacidade de resposta a incidentes de segurança. Tal como foi referido no âmbito do Treino, considerando a natureza dinâmica e abrangente das ameaças, a resposta eficaz aos incidentes passa muito por um conjunto de ações concertadas que ultrapassam frequentemente as fronteiras da organização. Considerando a natureza sensível das matérias relacionadas com a segurança da informação, as equipas de segurança das diferentes organizações tendem a operar de modo fechado, no entanto, existe cada vez mais a consciência de que só é possível uma resposta eficaz, trabalhando num ambiente cooperativo. A comunicação entre equipas de segurança de diferentes organizações, a partilha de conhecimento e de experiências, permite estabelecer relações de confiança, contribuindo para a um conhecimento global do que se passa no ciberespaço, permitindo estabelecer uma rede virtual de monitorização que tem como maior produto a produção de avisos antecipados que permitem agir de forma preventiva em relação a muitos ataques de natureza global. A estandardização de processos e uma taxonomia comum são fundamentais para que exista uma comunicação eficiente. Atualmente esse esforço está feito por todos através da constituição de encontros organizados entre equipas de segurança de diversas organizações, que é exemplo a nível nacional a rede de CSIRT[58].

[58] A Rede Nacional de CSIRT é um “fórum de cooperação entre equipas portuguesas de resposta a incidentes de segurança informática" que pretende fomentar "ações de sensibilização para a temática da segurança informática junto dos sectores da Banca, da Administração Pública e dos operadores de infraestruturas críticas nacionais" (...) reforçando "os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão”. (Computerworld, Rede Nacional de CSIRT quer sensibilizar e cooperação com autoridades, 2011), consultado em 12 de abril de 2015. As Forças Armadas portuguesas integram esta rede com o estatuto de "observadores".

4. Modelo para edificação da capacidade de resposta a incidentes de segurança da informação

Seguindo a linha orientadora da metodologia DOTMLPI-I que tem servido de base a este trabalho, pretende-se abordar os vários aspetos que compõem uma capacidade de resposta a incidentes de segurança da informação, no sentido de propor um modelo que seja aplicável à Marinha Portuguesa, mas que seja suscetível de ser extrapolado para outras estruturas organizacionais idênticas, quer ao nível da sua dimensão, quer na organização dos seus sistemas de informação[59].

Este modelo basear-se-á nas boas práticas e recomendações retiradas das normas e metodologias apresentadas no capítulo 2, da análise feita ao modelo adotado pela OTAN, e nas conclusões retiradas das entrevistas feitas aos especialistas, realizadas no capítulo 3.

Pretende-se que o modelo seja mais que uma compilação dos resultados obtidos, pelo que a sua proposta será também resultado da reflexão nesta área específica da segurança da informação.

4.1. Doutrina

Cumpre neste ponto a identificação inequívoca do objetivo que se pretende alcançar com a edificação da capacidade de resposta a incidentes de segurança da informação, bem como, qual a comunidade alvo que irá interagir com esta capacidade e os princípios e procedimentos que irão servir de base à sua ação. Como documentos basilares consideram-se a "Estratégia Nacional para Segurança no Ciberespaço" que apresenta por base a necessidade de garantir "*a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação*" (DR D. d., Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015, 2015), o despacho do ministro da Defesa n.º 13692/2013, no qual se publica a "Orientação Política para a Ciberdefesa", onde é claramente definida a necessidade de "*Garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques (…) e de contribuir de forma cooperativa para a cibersegurança nacional*". São ainda consideradas como doutrinárias as publicações militares PEMGFA 301 e PCA 16, já referidos anteriormente.

4.1.1. Objetivo

Pretende-se dotar a Marinha Portuguesa de uma capacidade de se preparar, detetar, reagir e recuperar de incidentes de segurança da informação que possam ocorrer no âmbito

[59] A Marinha Portuguesa possui uma infraestrutura tecnológica que apresenta uma dispersão geográfica que cobre todo o país (continente e ilhas), com mais de 50 locais diferentes onde funcionam vários organismos e entidades que utilizam a infraestrutura de comunicações e a rede de serviços disponibilizados pela Marinha. Entre estes serviços encontram-se os básicos como o correio eletrónico, o acesso à Intranet, à Internet e ainda várias aplicações e bases de dados fundamentais à operação dos serviços. Esta infraestrutura de comunicações e serviços é acedida por mais de 8000 utilizadores registados na estrutura de diretório. Existe ainda o apoio disponibilizado aos navios que se encontram em missão no mar, que através de comunicações por satélite disponibilizam os mesmos serviços aos utilizadores embarcados, independentemente do local e da hora em que se encontram. Para suporte de toda esta estrutura está edificada uma arquitetura de segurança e serviços, alojada num *Data Center* principal.

das suas infraestruturas de informação e comunicações, recolhendo as lições aprendidas, contribuindo para a Cibersegurança das infraestruturas TIC da Marinha e das Forças Armadas. A sua ligação direta ao Centro de Ciberdefesa permite-lhe contribuir também, para a Cibersegurança nacional, através da partilha de informação e de ações conjuntas a serem coordenadas por este órgão.

Atendendo à sua caraterística militar é também objetivo participar ativamente nas operações no Ciberespaço, seguindo as orientações operacionais do Comando Operacional da Marinha (Comando Naval) ou do Chefe do Estado Maior General das Forças Armadas.

4.1.2. Âmbito

A comunidade alvo da atuação desta capacidade são todas as Unidades e Organismos que utilizam os recursos informacionais e sistemas de informação da Marinha. Incluem-se neste conceito as unidades em terra, as unidades navais (mesmo que se encontrem a navegar com missão atribuída) e as entidades que, mesmo não pertencendo à Marinha, utilizem total ou parcialmente as suas infraestruturas TIC (eg, Autoridade Marítima).

4.1.3. Princípios e procedimentos

Um dos princípios que cumpre relevar é o da segurança ser da responsabilidade de todos, como tal existe o dever de informação sobre qualquer evento de segurança que seja detetado.

Para alcançar os objetivos a que se propõe, a Capacidade implementa um processo de gestão de incidentes baseado na norma ISO 27035 ao qual foram introduzidas alterações de modo a reforçar a importância de validação das respostas no processo iterativo da gestão dos incidentes. Na figura 13 está representado o ciclo de gestão de incidentes que se passa a descrever.

Figura 13 - Ciclo de gestão de incidentes (baseado na ISO/IEC 27035)

A fase de Preparação e Planeamento começa por fazer um levantamento exaustivo dos sistemas de informação a proteger, das infraestruturas que os suportam e de uma análise de vulnerabilidades. Segue-se a sua classificação em termos de criticidade para a organização, o modo como são geridos e operados e o planeamento dos mecanismos de ação para a monitorização dos eventos e resposta aos incidentes.

A maioria das condições de preparação e planeamento são distribuídas ao longo da análise DOTPMLF-I, pelo que em cada uma das dimensões serão referidas as mais relevantes.

O sucesso de uma correta preparação permite criar as condições para a operacionalização da fase de Deteção e respetivo registo dos eventos. Nesta fase procede-se à receção dos vários eventos de segurança provenientes das várias fontes. Independentemente da fonte que gerou o evento, seja de um equipamento de segurança, de comunicações ou o relato de um utilizador, todos os eventos devem ser corretamente registados (grupo data/hora, origem do relato, a sua descrição, quem o rececionou). O registo do evento numa base de dados assume particular importância, pois permitirá estabelecer relações entre eventos e entre eventos e incidentes.

Os eventos registados passam para a fase de Avaliação e Decisão onde através da sua análise são identificados como incidentes ou "falsos positivos". A avaliação deve ter em consideração a criticidade dos equipamentos e sistemas envolvidos, e a sua vulnerabilidade perante a natureza do incidente, esta avaliação irá permitir a categorização do incidente e atribuir-lhe a prioridade de resposta. Todas estas ações e decisões devem ser atualizadas na plataforma de registo.

Perante um incidente de segurança impõe-se uma resposta que tem por principal objetivo a resolução do incidente. Segue-se a reposição da normalidade dos serviços que eventualmente tenham sido afetados pelo incidente ou pelas ações que permitiram a sua recuperação. Finalmente é importante que se desenvolvam as ações necessárias à eliminação ou mitigação da vulnerabilidade que permitiu a ocorrência do incidente. Terminadas estas ações de resposta é importante fazer o controlo de qualidade das mesmas, assim, deve-se voltar à fase de deteção em busca dos indícios que demonstrem que as ações realizadas não só resolveram completamente o incidente, como corrigiram as vulnerabilidades que, de forma voluntária ou involuntária, lhe deram origem. Perante a confirmação da resolução do incidente, importa fazer o seu encerramento na plataforma de registo, com a descrição da ações realizadas e outras informações consideradas relevantes. Esta fase termina com a notificação do encerramento do processo às entidades responsáveis pelos sistemas afetados.

Segue-se a avaliação do modo como decorreu todo o processo, desde a deteção do evento à resposta ao incidente. Desta avaliação importa aferir se os processos adotados para a sua resolução foram os mais corretos, ou se de algum modo poderão ser otimizados. As conclusões e as lições aprendidas podem levar a propostas de alteração a introduzir na fase de preparação e planeamento que permitam à organização uma preparação mais adequada de proteção evitando futuros incidentes semelhantes. Caso se justifique, estas conclusões deverão ser partilhadas com outras organizações, nomeadamente com o Centro de

Ciberdefesa. No anexo G apresenta-se um *workflow* que mapeia as diferentes ações a realizar durante as várias fases do ciclo de gestão de incidentes.

4.1.4. Políticas de comunicação

A existência de uma política de comunicação é crucial em todo o processo de operacionalização de uma capacidade de resposta a incidentes.

Devem ser estabelecidos canais bem definidos que facilitem a interação entre a comunidade constituinte e o Núcleo de resposta a incidentes, que será objeto de uma apresentação detalhada mais adiante. Esta comunicação tem três vetores de informação principais. Primeiro há que considerar um mecanismo simples e de fácil acesso para o relato de incidentes de segurança, neste sentido apresentam-se como evidentes a divulgação de contactos telefónicos que permitam a comunicação direta entre quem deteta o evento e a equipa responsável pela "deteção e registo", um endereço de correio eletrónico exclusivo para este fim e um formulário eletrónico a disponibilizar na intranet da Marinha. No anexo F apresenta-se um exemplo de como estas e outras informações sobre o Núcleo RISI são disponibilizadas à organização, seguindo a RFC 2350[60]. Em segundo lugar considera-se relevante a existência de um sítio na intranet dedicado a esta temática, no qual sejam disponibilizadas informações relacionadas com incidentes de segurança a nível global, documentação com informação relativa à doutrina interna e externa, textos com recomendações e alertas de segurança internos e externos, algumas ferramentas de apoio para a eliminação de *malware* e o já referido formulário eletrónico que permita o relato de um evento de segurança. O terceiro vetor de informação a explorar é um boletim eletrónico, de periodicidade mensal, para divulgação geral dirigido à comunidade constituinte, apresentando informação estatística sobre os incidentes de segurança da informação que ocorrem nas redes de Marinha, acompanhado de recomendações importantes sobre a Cibersegurança na Marinha. Estes meios de comunicação interna ao permitirem e fomentarem a participação da comunidade na resposta aos incidentes, cumprem uma importante função de construção de uma consciência coletiva de Cibersegurança.

A resposta a incidentes de segurança da informação faz-se cada vez mais de forma cooperativa, atendendo à natureza holística das ameaças. Desta forma, a comunicação e a partilha de informação com parceiros externos, com os quais se estabeleceram previamente relações de confiança, é fundamental para o sucesso das fases de preparação e de resposta. Para que a troca de informação seja eficaz e eficiente, é importante que estejam acordados pontos comuns de entendimento, nomeadamente ao nível de uma taxonomia comum[61] para os

[60] A RFC 2350 apresenta a estrutura de um documento a ser divulgado junto da comunidade constituinte, com informação sobre a Equipa de Resposta a Incidentes de Segurança que a serve, nomeadamente sobre os objetivos, o âmbito das suas ações, a sua constituição, modos de contacto entre outras. (IETF, 1998), consultado em 21-05-2015.

[61] A Rede Nacional de CSIRT definiu na sua "Política de classificação de incidentes da Rede", o modo como os seus membros deveriam fazer a classificação dos mesmos tendo sido aprovada uma classificação baseada em 2 vetores – "Tipo de Incidente" e "Tipo de Evento", publicada num documento com a Taxonomia já acordada entre os membros. (RCTS R. C., 2015), consultado em 19-04-2015.

incidentes. No anexo E apresenta-se um exemplo de taxonomia comum para a classificação de incidentes de segurança publicado pelo CNCS, com base no documento elaborado pela Rede Nacional de CSIRT.

Para finalizar este ponto relativo às Políticas de Comunicação, importa que esteja bem definido o modo como o Núcleo de resposta a incidentes deve agir perante incidentes que de algum modo tenham repercussão mediática, ou quando a sua resolução implica intervir publicamente. Neste caso a comunicação deve ser feita pelo gabinete de Relações públicas da Marinha, que articulará com a entidade coordenadora, neste caso o Estado-Maior da Armada. Todas as comunicações para o exterior devem ser feitas de modo a preservar a imagem institucional da organização.

4.2. Organização

No que se refere à Organização, o modelo proposto segue de perto a estrutura adotada pelo NCIRC da OTAN, com 3 níveis distintos de intervenção. Um primeiro nível responsável pela governação e coordenação da Ciberdefesa da Marinha, um segundo nível essencialmente técnico e operacional onde se inclui a resposta a incidentes e um terceiro nível correspondente à comunidade constituinte, nomeadamente os responsáveis locais pela operação e segurança dos sistemas de informação. Na figura 14 apresenta-se o esquema de relações entre os diferentes níveis e destes com órgãos externos à CRISI da Marinha[62].

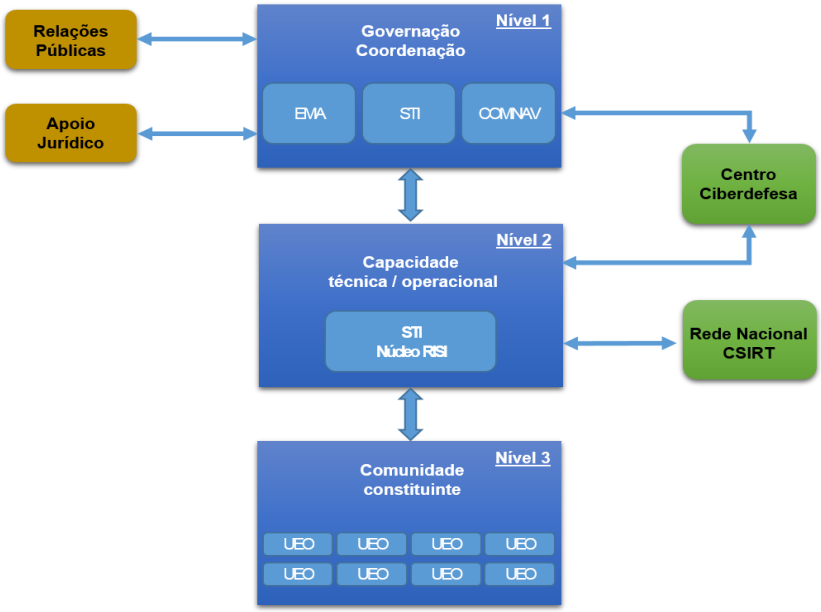

Figura 14 - Organização da Capacidade de Resposta a Incidentes de Segurança da Informação

No referente ao nível 1, as responsabilidades de governação e coordenação da capacidade são distribuídas por três entidades distintas, de acordo com a natureza das matérias a considerar. Ao Estado-Maior da Armada (EMA) compete a governação da Ciberdefesa, enquadrando-a com a Diretiva de Planeamento da Marinha, nomeadamente no que se refere à doutrina. Compete também ao EMA,

[62] A relação com as entidades externas será aprofundada no ponto dedicado à interoperabilidade.

através do Gabinete de Relações Públicas, a articulação com entidades externas às Forças Armadas que pretendam estabelecer contacto com a CRISI, avaliando que informação poderá ser alvo de divulgação pública ou que colaboração poderá ser estabelecida. No referente às necessidades de apoio jurídico, considerando a dimensão da estrutura associada à CRISI, considera-se que será mais adequado utilizar o já existente Departamento Jurídico de apoio ao Gabinete do Almirante CEMA, em detrimento de uma capacidade própria, para todas as questões de natureza jurídica que surjam no âmbito da ação da CRISI, como sejam a validação da legalidade das políticas a implementar ou no apoio a ações processuais que surjam na sequência de eventuais violações das normas e princípios estabelecidos para a utilização dos sistemas de informação da Marinha.

A Superintendência das Tecnologias da Informação (STI) é o órgão de Marinha responsável pela gestão do recurso Informação ao longo do seu ciclo de vida, garantindo a qualidade da informação utilizada na Marinha e ainda a eficácia e a segurança da infraestrutura CSI e dos serviços TI. Assim, no âmbito da CRISI, compete à STI a coordenação de toda a área técnica e de segurança dos sistemas de informação, nomeadamente a definição das políticas a implementar na Marinha para a exploração dos SI e a coordenação técnica da CRISI. A STI constitui-se como o ponto de contacto com o Centro de Ciberdefesa ou outras entidades externas para assuntos de natureza técnica da resposta a incidentes, podendo delegar esta responsabilidade na coordenação do Núcleo RISI.

Considerando a aplicação deste modelo a uma organização militar como a Marinha é expectável que seja também considerada a sua capacidade de conduzir operações no Ciberespaço. Atendendo à escassez de recursos humanos especializados e materiais, propõe-se o envolvimento dos recursos do Núcleo RISI nas operações militares a conduzir no Ciberespaço. Na Marinha compete ao Comando Naval (COMNAV) a condução das operações militares, desta forma o COMNAV surge como a entidade coordenadora das atividades operacionais de natureza militar da CRISI, servindo de ponto de contacto com o Centro de Ciberdefesa para assuntos de natureza operacional, nomeadamente a participação em exercícios de natureza cibernética ou de operações no ciberespaço.

O segundo nível de organização corresponde à capacidade técnica e operacional de intervenção da CRISI. Este nível de intervenção é materializado no Núcleo RISI, que para este fim deverá estar hierarquicamente dependente da STI. Considerando uma vez mais a escassez dos recursos humanos especializados, este poderá ser guarnecido com elementos que acumulem funções na Direção Técnica das TIC, sendo neste caso crítico assegurar a sua independência hierárquica e funcional dos respetivos Departamentos Técnicos. O Núcleo RISI tem a responsabilidade direta da gestão dos incidentes ao longo do seu ciclo de vida (ver figura 13), sendo responsável pelas ações a desenvolver em cada uma das fases anteriormente apresentadas. Para além das funções de monitorização e resolução de incidentes, o Núcleo, sob coordenação da STI, deverá garantir a capacidade de análise forense aos sistemas de informação, colaborando com as autoridades judiciais e militares. Finalmente, o Núcleo deve ter a capacidade de desenvolver operações no ciberespaço em coordenação com o COMNAV e o Centro de Ciberdefesa. No âmbito da resposta concertada a incidentes e em cooperação técnica com outras entidades, o Núcleo articula-se diretamente com o Centro de Ciberdefesa e com a Rede Nacional de CSIRT.

Para cumprir com as obrigações que lhe estão atribuídas, o Núcleo RISI apresenta uma organização interna baseada numa estrutura funcional. Assim, existe um nível de coordenação que será responsável por gerir as atividades técnicas e administrativas do Núcleo RISI e responder por este, perante as entidades coordenadoras. Segue-se um nível exclusivamente técnico, com grande conhecimento da organização e das suas infraestruturas TIC, responsável pela gestão incidentes. Terá de possuir valências que lhe permitam assegurar as funções necessárias à gestão do incidente, que incluem a sua triagem e classificação, fazer a sua investigação e reagir de modo a conseguir a sua resolução e a recuperação dos serviços afetados. Este nível deve ainda possuir capacidade de análise forense e de conhecimentos técnicos avançados de análise de *malware*. Por fim, existe um nível responsável pela monitorização dos eventos, que faz a receção de todos os relatos de incidentes e o seu registo na plataforma de gestão, atribuindo a responsabilidade de gestão do mesmo a um elemento do nível técnico[63]. Sob a orientação do coordenador do Núcleo NRISI, compete ainda a este nível a manutenção do *site* da CRISI e a elaboração dos boletins informativos periódicos, e a comunicação com a comunidade constituinte.

A Comunidade Constituinte diz respeito às Unidades, Estabelecimentos e Órgãos da Marinha (UEO) e representam o nível 3 da organização de resposta incidentes. Todas as UEO da Marinha possuem identificado na sua organização interna, um técnico responsável pela administração local da sua infraestrutura TIC. Este elemento constitui-se como o ponto de contacto para todos os assuntos relacionados com a segurança da informação no seu domínio local, colaborando na identificação e mitigação de vulnerabilidades, participando sob a coordenação do Núcleo RISI, como elemento ativo na resolução de incidentes e na implementação de políticas específicas de segurança[64].

4.3. Treino

O treino surge sempre como uma das áreas essenciais quando se procura estabelecer e manter uma capacidade operacional eficaz e eficiente. Neste contexto é importante que o Treino permita testar toda a cadeia de decisão, os processos de comunicação envolvidos na resposta a incidentes, a preparação técnica das equipas e finalmente o seu funcionamento em ambientes de grande pressão psicológica. A execução de ações de treino num ambiente de grande realismo permitem melhorar a capacidade de resposta a incidentes de segurança da informação, a identificar lacunas de formação técnica, eventuais falhas nos processos organizacionais e de comunicação, constituindo-se assim como uma oportunidade importante de melhorar o desempenho. Através da análise rigorosa dos resultados das ações de treino, podem surgir propostas de revisão dos processos, da formação técnica, ou mesmo da própria organização.

[63] Numa primeira ação, a atribuição de responsabilidade sobre o evento poderá ser feita ao elemento da equipa técnica que aparente ter menos eventos atribuídos, sem prejuízo de posteriormente o coordenador do NRISI alterar esta atribuição para outro elemento que considere mais indicado, quer por formação técnica, quer por gestão de pessoal.

[64] A grande maioria das políticas de segurança são transversais a toda a Marinha, sendo aplicadas de forma centralizada através Políticas Globais de Domínio, no entanto, considerando a multiplicidade de UEO e de diferentes missões, existem exceções que é importante manter controladas.

Nesta dimensão, o modelo proposto aproveita as ações de treino existentes a nível nacional e internacional. Atendendo à sua característica militar, o objetivo primário é garantir a participação do Núcleo RISI, sob coordenação do COMNAV e em articulação com o Centro de Ciberdefesa, no exercício anual da OTAN "Cyber Coalition" que, como vimos anteriormente, tem como objetivos principais de treino a Capacidade de Decisão, a Coordenação, a Partilha de Informação e o treino das Capacidades Técnicas (NATO, CC14 Training Objectives, 2014). A nível nacional, atendendo ao facto de, quer o CNCS quer o CDD estarem numa fase inicial de operacionalidade, não existem ainda exercícios de natureza Ciber que envolvam toda a comunidade nacional, neste caso particular destaca-se o exercício de ciberdefesa do exército português, o Ciber Perseu[65], que nas suas edições mais recentes de 2013 e 2014, tem sido aberto à participação dos outros ramos das forças armadas e da comunidade civil, sendo por isso também uma oportunidade de treino importante a considerar para o Núcleo RISI da Marinha.

Os exemplos de treino anteriormente indicados, propostos neste modelo para participação do Núcleo RISI da Marinha, são excelentes oportunidades de treinar e avaliar o desempenho das equipas, mas de certo modo restritas à participação da comunidade mais diretamente envolvida na capacidade de resposta a incidentes de segurança da informação. Neste campo, a ação do Núcleo RISI da Marinha não deve ficar restringida às ofertas que aparecem do exterior, sendo seu objetivo preparar e organizar oportunidades de treino internas que envolvam toda a comunidade naval, levando a oportunidade de treino até às UEO, ou seja, até aos utilizadores dos sistemas de informação da Marinha.

4.4. Material

Neste campo existem alguns pressupostos que são essenciais ao sucesso da missão. O Núcleo RISI deve ter ao seu dispor ferramentas que lhe permitam assegurar a resposta a incidentes de segurança da informação, quer nos segmentos onde circulam informação Não Classificada, quer nos segmentos de rede classificados. Importa ter em consideração que devido à diferença de níveis do grau de segurança da informação, terão de ser consideradas soluções segregadas fisicamente para a monitorização e registo dos incidentes.

O Núcleo RISI terá de possuir a capacidade de monitorização de todas as plataformas de segurança que protegem os SI da Marinha, assumindo aqui um papel fundamental a existência de um equipamento do tipo SIEM que assegure a correlação dos eventos recebidos das diversas plataformas. Igualmente crítico é a existência de uma plataforma que permita o registo dos eventos de segurança, o seu eventual escalar para incidente, o registo de todas as ações realizadas pela equipa no seguimento/tratamento deste evento/incidente deste a sua deteção à sua resolução. São também importantes os meios de comunicação que permitem o contacto com a comunidade constituinte, entre os diferentes níveis da capacidade de resposta a incidentes e com as outras equipas externas de

[65] O exercício Ciber Perseu apresenta como objetivos "testar os procedimentos técnicos e operacionais de resposta a ciberataques existentes no Exército, assim como avaliar os mecanismos de Cooperação com Entidades e Organizações externas ao Exército" (Exercito, 2014), consultado em 09/05/2015.

resposta a incidentes de segurança (CSIRT) com as quais existam relações de confiança.[66] Para que seja possível acompanhar os incidentes desde a sua origem, é fundamental a existência de ferramentas que permitam identificar vulnerabilidades, ferramentas para recolha e análise tráfego de rede e em muitos casos fazer a recolha e análise de artefactos (eg, disco rígidos de computadores).[67] No seu todo, estamos perante um conjunto de ferramentas que representam um significativo investimento de recursos financeiros da organização, desta forma é importante ter em consideração a própria arquitetura dos sistemas de informação e a compatibilidade entre as várias plataformas, de modo garantir a sua interoperabilidade e a rentabilizar ao máximo a sua aquisição.

4.5. Liderança

Tendo sido proposto anteriormente para este modelo, a separação das questões de coordenação da capacidade, dos aspetos essencialmente técnicos da resposta a incidentes, nomeadamente tendo sido consideradas para o efeito, entidades com responsabilidades na gestão superior da Marinha, aspeto que se considera essencial para o posicionamento desta capacidade no interior da organização, apresenta-se aqui a liderança na perspetiva da coordenação técnica/operacional do Núcleo RISI.

O líder deste grupo deverá ser alguém com reconhecidas capacidades técnicas, de coordenação do trabalho em equipa, com bastante experiência e que possua um conhecimento atualizado dos problemas relacionados com a segurança da informação. Como elo de ligação com o nível superior de decisão da organização, terá de possuir um elevado conhecimento organizacional e ser reconhecido pela sua responsabilidade. Como gestor da capacidade técnica do núcleo, deve ter um profundo conhecimento dos elementos da sua equipa, quer ao nível técnico quer humano, dos seus pontos fortes e das suas fragilidades, de modo a poder escolher as pessoas certas para a resolução dos diversos tipos de incidentes. Baseado na sua experiência, capacidade e formação, este deve ter o poder de decisão sobre a gestão dos incidentes, nomeadamente no seu escalonamento para outras entidades, assumindo-se como ponto de contacto com entidades externas à Marinha, para assuntos de natureza exclusivamente técnica e constituindo-se como uma referência para os outros elementos da equipa.

Idealmente, na estrutura do Núcleo RISI da Marinha, o líder deve ser um oficial superior com uma forte formação e experiência técnica. No próximo ponto dedicado ao Pessoal será analisado com maior detalhe a formação do líder.

[66] No caso particular das comunicações entre equipas de segurança, é importante poder manter a confidencialidade das comunicações, sendo por isso necessário utilizar mecanismos de encriptação dos canais de troca de informação.

[67] A recolha de evidências sobre os incidentes ou as causas que os provocaram deve ser feita de acordo com os procedimentos legais de "recolha de prova", para que a informação recolhida seja suscetível de ser utilizada em eventuais processos de natureza disciplinar ou legal.

4.6. Pessoal

Sendo esta uma das dimensões mais críticas na construção da capacidade de resposta a incidentes, o foco estará na seleção de elementos confiáveis, com perfil para trabalhar em equipa em situações de *stress*, com as competências necessárias, e a formação adequada para a execução das diversas tarefas associadas a esta capacidade. Na realidade, numa organização governamental como a Marinha Portuguesa, em que o recrutamento está muito restringido aos elementos dos seus atuais quadros de pessoal, pode ser difícil identificar os elementos que agreguem todos estes fatores e capacidades para a construção da equipa, assumindo por isso especial relevância o envolvimento da Direção de Pessoal, na escolha dos indivíduos que potencialmente apresentam o perfil adequado, devendo este ser confirmado num período de adaptação a realizar, inserido nas atividades do Núcleo RISI. Para a realização com sucesso das tarefas associadas ao ciclo de gestão de incidentes já apresentado na figura 13, os vários elementos que constituem o Núcleo terão de desempenhar diversos papéis, aos quais estão associadas competências específicas, às quais por sua vez correspondem determinados níveis de formação académica e técnica de acordo com o sistema nacional de qualificações[68]. Do ponto de vista de credenciação de segurança, atendendo a que o Núcleo RISI é responsável pelos segmentos Classificados e Não Classificados da rede, todos os elementos devem ser credenciados em Nacional Secreto e NATO Secret.

4.6.1. Monitor de Incidentes

Estes elementos têm por principal função a monitorização dos eventos nas plataformas de segurança, na plataforma de correlação de eventos e a receção das notificações que tenham origem na comunidade constituinte (notificações recebidas por correio eletrónico ou via plataforma *web*). Todos os eventos detetados e notificações recebidas devem ser registados na plataforma de gestão de incidentes, devendo esta ser preenchida com o máximo de informação existente. Compete ainda aos Monitores de Incidentes participar nas tarefas administrativas relacionadas com a atividade do Núcleo RISI, nomeadamente na recolha e tratamento dos dados para fins estatísticos, colaborar na recolha de informação para a elaboração do boletim informativo periódico e manutenção do sítio na intranet da CRISI.

Estes elementos são oriundos do quadro de praças, com formação interna específica em informática (administração de sistemas e de redes) e também em INFOSEC. Estes elementos devem possuir o nível IV de qualificação.

[68] Os níveis aqui considerados são os apresentados na Portaria n.º 782/2009 referentes ao Sistema Nacional de Qualificações, que nivela as qualificações de acordo com uma matriz de "conhecimentos, aptidões e atitudes", resultando estes numa tradução para níveis de educação e formação. (DR D. d., Quadro Nacional de Qualificações, DR, 1.ª série — N.º 141 — 23 de Julho de 2009 , 2009).

4.6.2.Gestor de Incidentes

Estes indivíduos têm a responsabilidade de gerir o incidente desde que este é introduzido na plataforma até à sua resolução final. Cada um dos incidentes registados na plataforma deve ser assumido por um gestor de incidentes, podendo este ter vários incidentes em aberto à sua responsabilidade. Não havendo indicação em contrário por parte do Coordenador do Núcleo, os incidentes registados são distribuídos pelos Gestores de Incidentes por ordem de chegada ao sistema. Compete ao Gestor do Incidente fazer uma primeira triagem para confirmar que estamos efetivamente perante um incidente, e em caso afirmativo, iniciar a sua investigação. Caso o incidente não seja validado como tal, deve encerrar o incidente na plataforma de gestão, com indicação sobre o porquê da sua não consideração como incidente e com eventuais instruções de notificação para ação dos Monitores de Incidentes. O Gestor de Incidente, no âmbito da sua investigação, pode solicitar apoio aos Analistas Forenses para a resolução do incidente ou para análise de vulnerabilidades e proposta de soluções de mitigação. Se for considerado necessário escalar a investigação do incidente para entidades externas à Marinha, essa necessidade deve ser comunicada ao Coordenador do Núcleo que determinará as ações subsequentes. Tendo sempre em consideração a sua disponibilidade, o Coordenador do Núcleo pode solicitar a sua colaboração nas tarefas administrativas relacionadas com a atividade do Núcleo RISI.

Estes elementos são oriundos da classe de sargentos, com formação interna técnica específica nas áreas de administração de sistemas, de comunicações de redes e de INFOSEC, complementada com formação técnica avançada sobre gestão de incidentes e de segurança informática, no exterior da Marinha. Estes elementos devem possuir o nível V de qualificação.

4.6.3.Analista Forense

O Analista Forense tem por principal função auxiliar a investigação dos incidentes quando esta exige um conhecimento técnico muito mais profundo. As suas valências técnicas permitem-lhe fazer um estudo detalhado, recorrendo a análise forense na área de redes e sistemas de informação, das vulnerabilidades que permitiram a ocorrência do incidente e propor ações de mitigação para a correção dessas vulnerabilidades, sejam estas de natureza estritamente técnica ou ao nível dos processos. Deve colaborar diretamente com o Gestor do Incidente, para após a resolução do incidente fazer uma reavaliação das medidas tomadas, validando assim a sua eficácia em ambiente real. Compete ao Analista Forense apoiar o Coordenador do Núcleo RISI na análise e elaboração de propostas aos níveis superiores de coordenação, para a edificação ou revisão de processos e procedimentos que estejam estabelecidos doutrinariamente. O Núcleo RISI colabora com os outros órgãos da Marinha ou Ramos das Forças Armadas no âmbito da segurança da informação e da

gestão de incidentes, de acordo com as necessidades de apoio técnico especializado manifestadas, sendo responsabilidade do Analista Forense apoiar o Coordenador do Núcleo na representação da CRISI nessas situações (eg: colaboração com a Inspeção Geral de Marinha ou a produção de pareceres técnicos na área da segurança da informação).

Estes elementos são oriundos do quadro de oficiais subalternos, possuindo uma forte formação técnica (superior) nas áreas da Segurança da Informação, Infosec, Gestão de Incidentes e Investigação Forense. Estes elementos devem ter um nível de qualificação mínimo de nível VI sendo desejável o nível VII.

4.6.4.Coordenador do Núcleo

O Coordenador tem por principal função a gestão diária do funcionamento do Núcleo RISI. Deve acompanhar de perto o desempenho dos diferentes níveis de operação do Núcleo, tendo a preocupação de garantir uma equitativa distribuição de tarefas e que os incidentes estão a ser geridos pelos indivíduos mais adequados, atendendo a natureza do incidente. Deve garantir um planeamento adequado de formação para os diversos elementos, de acordo com as suas capacidades e valências, procurando dentro do possível a homogeneização das equipas, mas dando espaço de progressão aos que demonstrarem maior potencial. O Coordenador do Núcleo RISI representa-o perante os níveis superiores de Coordenação e perante as entidades externas da Marinha. Compete-lhe garantir a produção periódica dos boletins informativos da CRISI, a gestão e manutenção do sítio da CRISI na Intranet e a organização de eventos de divulgação na área da segurança da informação. O Coordenador do Núcleo RISI deve reunir periodicamente com os elementos da equipa para análise e discussão do evoluir dos tipos de incidentes e dos procedimentos estabelecidos para a sua resolução. É o responsável por apresentar superiormente sugestões de alteração ao normativo existente relacionado com a segurança da informação.

Este elemento deve ser um oficial superior, com elevada formação técnica (superior) nas áreas de Segurança da Informação, INFOSEC e com grande experiência e formação na Gestão de Incidentes. Este elemento deve ter um nível de qualificação de nível VII.

Como apresentado, para a organização do Pessoal do Núcleo RISI é proposto um modelo de funcionamento em quatro níveis, que se considera como o mais adequado ao cumprimento da sua missão, tendo por base os papéis definidos pela ENISA no seu guia de boas práticas (ENISA, Good Pratice Guide For Incident Management, 2010) e na experiência pessoal do autor baseada na participação em vários exercícios de Ciberdefesa da OTAN como sejam os *Cyber Coalition*. No que se

refere aos seus quantitativos, assumido o objetivo de ter uma capacidade de operação em permanência[69] o número de elementos a considerar será o seguinte:

- 1 (um) Coordenador do Núcleo RISI;
- 2 (dois) Analistas Forenses;
- 3 (três) Gestores de Incidentes;
- 8 (oito) Monitores de Incidentes[70].

Numa fase inicial de operação poderá ser difícil garantir a existência de pessoal em número suficiente com as qualificações necessárias. Considerando um período de formação inicial, é expectável que este quadro de pessoal apenas esteja disponível no final de 3 a 4 anos de operação. Desta forma, durante a fase inicial de operacionalização, poderá não ser possível garantir um funcionamento em permanência, sendo garantido o funcionamento apenas durante as horas normais de serviço, sem prejuízo de perante um incidente grave ou a necessidade de participar em exercícios, estender o seu funcionamento durante mais tempo. Considerando ainda o restringimento ao nível do pessoal numa fase inicial, os elementos existentes poderão ter de acumular funções, ou seja, os Gestores de Incidentes poderão exercer também a função de Monitores, os Analistas Forenses as funções de Gestores de Incidentes e mesmo o cargo de Coordenador do Núcleo poderá ser desempenhado em acumulação pelo Analista Forense com a posição hierárquica mais elevada.

4.7. Infraestruturas

Neste ponto são definidas as características físicas e de segurança do espaço no qual irá operar o Núcleo RISI. Competindo ao Núcleo RISI recolher, analisar e guardar informação sobre os eventos que ocorram nos vários segmentos de rede da Marinha, nomeadamente sobre os segmentos que transportam e processam informação classificada, assume especial importância as questões de segurança física e lógica. Como organismo inserido na estrutura de defesa do Estado, serão seguidas as instruções doutrinárias estabelecidas nas "normas destinadas a garantir a segurança protetiva das matérias classificadas de âmbito governamental contra ações de sabotagem e espionagem e, ainda, a evitar falhas humanas suscetíveis de ocasionar comprometimentos e quebras de segurança" (DR D. d., 1988)[71], nomeadamente no que se refere aos assuntos de segurança de pessoal, de segurança física[72] e de segurança da informação.

[69] As limitações de pessoal à constituição de um Núcleo RISI de grandes dimensões, levam a assumir que uma capacidade de operação em permanência (funcionamento de 24h x 7 dias por semana, ao longo de todo o ano), seja garantida apenas ao nível permanente na monitorização dos sistemas, ficando os níveis de gestão de incidentes e análise forense num regime de ativação "*on call*", de acordo com as necessidades identificadas.

[70] O número elevado de Monitores de Incidentes é justificado por estes elementos terem de assumir um funcionamento por turnos.

[71] SEGNAC 1 – Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas.

[72] O SEGNAC 1 apresenta uma divisão de classificação dos espaços físicos de acordo com a necessidade de proteger a informação conforme os seus diferentes graus de classificação. A CLASSE 1 apresenta especiais requisitos de segurança, pois corresponde a espaços onde se trabalha com informação de grau CONFIDENCIAL ou superior, assumindo-se que o acesso ao espaço físico permite também o acesso à informação.

No SEGNAC 4, especialmente dedicado à Segurança Informática, são detalhadas as medidas de segurança física das instalações (DR D. d., SEGNAC 4 - Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática, 1ª Série, nº 49 de 28-02-1990, 1990). Desta forma o Núcleo RISI deverá operar num espaço que cumpra os requisitos de segurança física de CLASSE 1 e no aplicável, implementar as medidas de segurança constantes no SEGNAC 4 como sejam, a "localização e estrutura das instalações", a "segurança elétrica", a "climatização", a "proteção contra incêndios", a "proteção contra radiações eletromagnéticas", o "controlo de entradas e saídas", entre outras.

De modo a estruturar e sistematizar a aplicação das várias medidas de segurança, "*prevenindo o acesso físico não autorizado os danos e as interferências na informação e nos recursos de processamento de informação da organização*" (ISO/IEC, ISO 27001 - Tecnologia de informação, Técnicas de segurança, Sistemas de gestão de segurança da informação – Requisitos, 2013) nas suas várias vertentes, e ainda "*a perda, dano, furto ou comprometimento de ativos e interrupção das operações da organização*", mencionadas também na norma ISO 27001, o Núcleo RISI seguirá um conjunto de controlos selecionados para a Segurança Física e Ambiental que se enumeram na tabela 12:

Objetivo	Controlo
Perímetro de segurança física	Devem ser definidos e utilizados perímetros de segurança para proteger as áreas que contenham informação sensível ou crítica e recursos de processamento de informação.
Controlos de entrada física	As áreas seguras devem ser protegidas através de controlos de entrada apropriados que assegurem que apenas é permitido o acesso a pessoas autorizadas.
Segurança em escritórios, salas e instalações	Devem ser concebidas e aplicadas medidas de segurança física para escritórios, salas e instalações.
Proteção contra ameaças externas e ambientais	Devem ser concebidas e aplicadas medidas de proteção física contra desastres naturais, ataques maliciosos ou acidentes.
Trabalhar em áreas seguras	Devem ser concebidos e aplicados procedimentos para trabalhar em áreas seguras.
Colocação e proteção de equipamentos	Os equipamentos devem ser colocados e protegidos de forma a reduzir os riscos de ameaças e perigos ambientais, e as oportunidades para acesso não autorizado.
Serviços básicos de suporte	Os equipamentos devem ser protegidos contra interrupções de energia elétrica e outras falhas causadas pelos serviços básicos de suporte.
Segurança da cablagem	A cablagem elétrica e de telecomunicações que transporta dados ou que suporta os serviços de informação deve ser protegida contra interceção, interferência ou dano.

Tabela 12 - Objetivos e controlos de segurança Física e Ambiental a implementar no Núcleo RISI (ISO/IEC 27001)

Concluindo, as Infraestruturas necessárias para a edificação desta capacidade, resumem-se na disponibilização de um espaço físico que garanta as necessárias condições de segurança física e ambiental de acordo com o nível da classificação da segurança processada, bem como os espaços necessários para a operação do Núcleo RISI, ou sejam os espaços que proporcionem adequadas condições de habitabilidade ao pessoal (vestiários, instalações sanitárias, espaço de lazer), espaços de trabalho (gabinetes), uma sala de maiores dimensões para a monitorização dos sistemas, uma sala de reuniões e os polos técnicos para alojamento do *hardware* de apoio às operações.

4.8. Interoperabilidade

As ameaças à qualidade da informação e aos próprios sistemas que a produzem e operam, caracterizam-se pela sua natureza dinâmica e pela acentuada imprevisibilidade dos seus vetores de ataque. Esta constatação faz com que uma efetiva capacidade de resposta a Incidentes de Segurança da Informação apenas seja possível num ambiente de defesa cooperativo, em que os vários intervenientes no esforço de proteção da informação, sejam estes de natureza estatal, privada, ao nível de um grande grupo económico ou das universidades, passando forçosamente pelas Forças Armadas, colaboram uns com os outros num esforço de construção de um conhecimento situacional do Ciberespaço Nacional.

A capacidade de resposta a incidentes de segurança da informação proposta neste modelo materializa-se na ação do seu Núcleo de RISI, que terá de assegurar as condições de interoperabilidade com os Núcleos dos outros Ramos da Forças Armadas, com o Centro de Ciberdefesa e através deste ou diretamente, com os elementos da rede de CSIRT e com o próprio Centro Nacional de Cibersegurança, não esquecendo a articulação com as diretivas recebidas da OTAN oriundas do NCIRC. A figura 15 representa as linhas de interoperabilidade estabelecidas entre os diversos atores envolvidos na resposta a incidentes de segurança da informação.

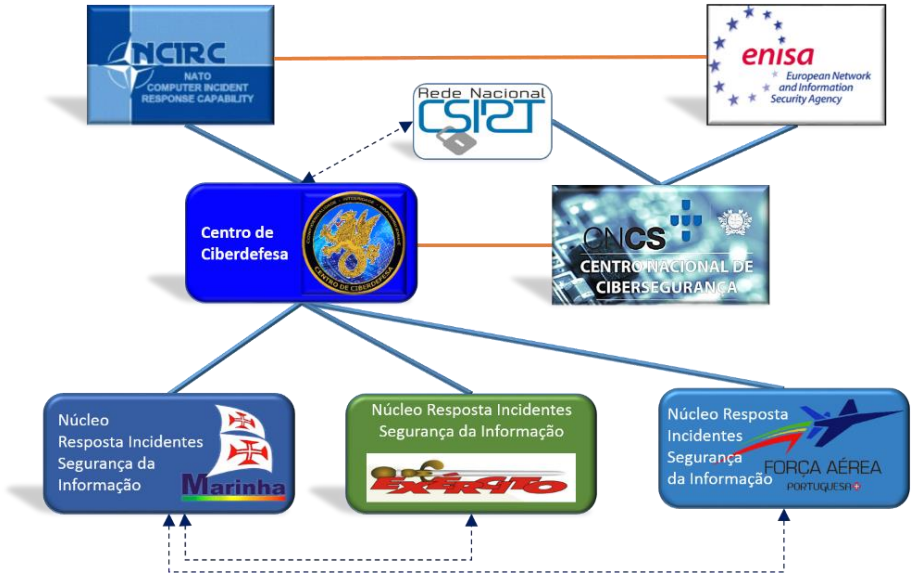

Figura 15 - Relações de Interoperabilidade do Núcleo RISI da Marinha

Para que as mais-valias trazidas pela interoperabilidade, como a capacidade melhorada de *inteligência,* conseguida através da partilha de informação absolutamente necessária para se conseguir agir em antecipação, para além das imprescindíveis relações de confiança, importa utilizar uma terminologia comum, modelos de dados compatíveis e uma estruturação da informação tão semelhante quanto possível. Com o propósito de assegurar estas condições, neste modelo propõe-se a utilização da plataforma *Request Tracker for Incident Response* (RTIR), já adotada pelo Centro de Ciberdefesa e bastante popular entre a comunidade de CSIRT nacionais, que já inclui todo um *workflow* de gestão dos incidentes. Como complemento, o Núcleo RISI adotará também a taxonomia divulgada pelo Centro de Cibersegurança de modo a facilitar a interação com os outros CSIRT.

Para desenvolver a Interoperabilidade, o Núcleo RISI prevê a sua participação ativa na organização e desenvolvimento de ações de divulgação e grupos de trabalho multidisciplinares, sobre os vários aspetos relacionados com a Cibersegurança e a Gestão de Eventos de Segurança, quer no âmbito da OTAN ou da sociedade civil.[73]

[73] A OTAN possui vários projetos de investigação a decorrer sobre questões da Cibersegurança, incluindo as relacionadas com a Interoperabilidade. Destaca-se o projeto "Multi National Cyber Defence 2 (MN CD2)", dedicado ao desenvolvimento de sistemas facilitadores da coordenação das ações de Ciberdefesa. Neste projeto está em desenvolvimento a plataforma Cyber Information and Incident Coordination (CIICS) que permite a "troca eficiente de informação não classificada mas potencialmente sensível sobre incidentes (incluindo informação sobre *malware*) entre os Computer Security Incident Response Teams (CSIRT) nacionais" (MNCD2, 2015), consultado em 17-5-2015.
Ainda no campo da Interoperabilidade a OTAN desenvolveu a plataforma Malware Information Sharing Platform (MISP), aberta à participação da comunidade com as quais estão estabelecidas relações de confiança. Esta plataforma web permite o acesso partilhado a uma base de conhecimento sobre *malware.* "Sempre que possível providencia mecanismos automáticos para importação e exportação de dados para outros sistemas. O objetivo é acelerar a deteção de incidentes e a produção de contramedidas de defesa, em especial para *malware* que não é bloqueado pela ação dos antivírus, ou faz parte de tentativas sofisticadas e direcionadas de intrusão (NCIA, 2015), consultado em 17-5-2015.

5. Conclusões

Este trabalho de investigação em Segurança da Informação e Direito no Ciberespaço tem como objetivo a definição de um modelo para a edificação de uma Capacidade de Resposta a Incidentes de Segurança da Informação.

Foi utilizada uma abordagem baseada nos conceitos empregues na OTAN para a edificação de novas capacidades operacionais. O estudo realizado centra-se em torno de um conjunto de dimensões diferentes, que no seu todo permitem uma análise holística do problema, identificando os elementos críticos para o sucesso da missão e as potenciais vulnerabilidades que possam existir. Essas dimensões são a Doutrina, a Organização, o Treino, o Material, a Liderança, o Pessoal, as Infraestruturas e a Interoperabilidade.

Na primeira parte abordou-se a problemática das ameaças cibernéticas e o modo como estas podem comprometer a segurança da informação das pessoas, dos estados e mesmo de infraestruturas que servem de apoio a serviços críticos para a sociedade. Esta constatação relevou a necessidade de se edificarem estruturas militares e civis com o objetivo de proteger a qualidade da informação, preparando a proteção dos sistemas de informação, monitorizando, analisando e detetando eventos relativos à operação dos sistemas, suscetíveis de se tornarem em incidentes, ou seja, estruturas com capacidade de resposta a esses incidentes e de recuperação dos sistemas.

A análise de várias normas e metodologias existentes como a ISO/IEC 27000 (27002 e 27035), a gestão de processos do ITIL, a organização apresentada pelo NIST ou o guia de boas práticas da ENISA, relacionados com a gestão de incidentes, permitiu identificar pontos comuns na abordagem a esta problemática, demonstrando a necessidade de existência de uma *framework* iterativa, com várias fases perfeitamente definidas, fundamentais para a construção do modelo apresentado.

Este trabalho pretendeu apresentar-se como inovador na abordagem das questões relacionadas com a Cibersegurança, ao fazê-lo numa perspetiva DOTMLPI-I. Para melhor enquadrar o tema nesta perspetiva realizou-se a análise da Capacidade de Resposta a Incidentes de Segurança Cibernética da OTAN, ao longo das várias dimensões. Esta análise permitiu identificar os vários aspetos relacionados com a edificação de uma capacidade desta natureza, as suas componentes mais críticas e antecipar alguns dos problemas que podem surgir durante a sua edificação. Evidenciou-se que existem dimensões que estão fortemente relacionadas entre si, como a Doutrina, a Organização e a Liderança, o Pessoal e o Treino. A identificação destas relações, os seus pontos fortes e as suas vulnerabilidades, contribuíram decisivamente para a estrutura apresentada no modelo e para a antecipação das dificuldades que possam surgir na sua edificação.

Com o objetivo de enriquecer a informação apresentada e com a preocupação principal de o modelo proposto apresentar uma elevada adesão à realidade, realizaram-se um conjunto de entrevistas escritas, a profissionais de reconhecida capacidade na área da Cibersegurança. Foi-lhes solicitado que analisassem a problemática da Resposta a Incidentes de Segurança da Informação, tendo a entrevista sido orientada num conjunto de questões que seguiram a abordagem DOTMLPI-I. Realizou-se a análise de conteúdo das referidas entrevistas e os resultados obtidos a partir da opinião do eng. Lino Santos (CNCS), do eng. Gustavo Neves (RCTS, ex-CERT.PT) e do eng. Santos Coelho (CDD), tendo estas

se constituído como um contributo decisivo, para as opções realizadas na elaboração do modelo proposto.

Conclui-se este trabalho de investigação com a apresentação efetiva de um modelo que permite a edificação de uma capacidade de resposta a incidentes de segurança da informação. A abordagem DOTMLPI-I mostrou-se bastante eficaz na identificação dos elementos chave para construção de uma estrutura organizacional desta natureza, com uma forte componente operacional. Permite ainda identificar quais os elementos que se podem apresentar como críticos na sua construção, ao mesmo tempo evidenciam os maiores riscos que se apresentam à sua concretização, como sejam, por exemplo, a necessidade de possuir quadros competentes (em numero e com formação adequada) para o desempenho das funções exigidas para a implementação da capacidade.

O modelo proposto apresenta uma forte componente prática nas soluções que recomenda implementar, como resultado do contributo dos especialistas entrevistados e da própria experiência do autor. Deste modo, o modelo foca-se na sua aplicação a uma estrutura organizacional como a Marinha Portuguesa, acreditando-se que poderá ser facilmente extrapolado para outros organismos estatais ou empresas, que apresentem uma dimensão e estrutura não muito diferentes da Marinha. Acompanhando as linhas diretoras da abordagem DOTMLPI-I são apresentados os Objetivos e o Âmbito, em conjunto com os Princípios e Procedimentos inerentes a uma capacidade deste tipo. É definida ainda uma organização que permite fazer a gestão da própria capacidade, de acordo com os objetivos superiormente definidos, ao separar claramente as funções técnicas da resposta a incidentes, da gestão superior e mesmo das unidades operacionais subjacentes. O modelo apresenta várias dimensões diretamente relacionadas com o pessoal, que vão desde a liderança, à formação e treino dos quadros, apresentando também as diferentes capacidades diretamente ligadas às funções a desempenhar. São também identificadas as particularidades da estrutura física dos espaços e dos meios materiais necessários à implementação de um Núcleo de RISI. O modelo conclui com o levantamento das entidades que participam de forma cooperativa na resposta a incidentes, salientando os mecanismos que permitem assegurar a Interoperabilidade.

De relevar que a Interoperabilidade está também diretamente relacionada com um dos eixos principais da orientação estratégica nacional para a segurança no ciberespaço, a Cooperação. Neste trabalho foram identificados como elementos chave para a Interoperabilidade, a existência de canais de comunicação confiáveis entre os elementos dos diferentes Núcleos RISI, a construção de relações de confiança e a utilização tanto quanto possível de processos comuns. Deste modo constitui-se como necessária a utilização de uma taxonomia comum, a normalização de procedimentos e do modelo de dados adotado. Considera-se que um dos principais meios para atingir este objetivo de Interoperabilidade é através de ações que impliquem a cooperação entre os diversos atores, com vista a atingir um objetivo comum. Indica-se como exemplo destas ações, o participar em vários *fora* e grupos de trabalho relacionados com temas de interesse comum, como sejam a segurança dos sistemas de informação, o cibercrime, a ciberdefesa ou a participação em exercícios de Cibersegurança / Ciberdefesa que impliquem uma interação entre os membros desta comunidade.

5.1. Trabalho futuro

Durante a fase de construção do modelo foi identificada a necessidade de se estabelecerem percursos formativos para os elementos que integram o Núcleo RISI, de acordo com as competências necessárias à operação da equipa de resposta a incidentes. No modelo foram identificados quatro perfis distintos, o Coordenador, o Analista Forense, o Gestor de Incidentes e o Monitor de Eventos. Foram genericamente indicados os níveis de qualificação necessária para o desempenho destas funções, no entanto considera-se importante que seja feito um estudo detalhado sobre as competências necessárias para cada uma delas e associa-las a percursos educativos, nos diferentes níveis, que permitam habilitar e certificar os indivíduos para o seu desempenho. Não se conhece nenhuma oferta educativa existente para esta área que cubra os vários níveis de qualificação, indicando-se como proposta de trabalho futuro a definição de um projeto educativo, multinível, eventualmente de natureza modular[74], que permita preparar os técnicos necessários, para o desempenho de funções num centro de resposta a incidentes de segurança da informação.

Outro aspeto do modelo que se considera oportuno para um estudo mais profundo, está relacionado com os mecanismos de comunicação e a estandardização dos processos, associados à imprescindível interoperabilidade entre os diversos atores que contribuem para a Cibersegurança. Atualmente cada entidade utiliza as suas próprias ferramentas de registo, faltando uma ferramenta de trabalho que seja consensual, que garanta canais de comunicação seguros, que facilite a classificação e o registo de incidentes, que seja interoperável e que contribua para a criação de uma verdadeira rede de inteligência entre a comunidade de resposta a incidentes. A rede nacional de CSIRT tem apostado em diferentes ferramentas *open source* para cumprir este objetivo e a União Europeia e a OTAN têm apoiado projetos de desenvolvimento de ferramentas com este propósito. Considera-se assim oportuno o acompanhamento das iniciativas nacionais e internacionais de desenvolvimento de ferramentas colaborativas para apoio a esta capacidade.

Finalmente, este trabalho apresenta um modelo de edificação de uma capacidade de resposta a incidentes de segurança da informação que carece de validação prática. Propõe-se como elemento de estudo futuro, o acompanhamento da aplicação do modelo a um caso concreto e assim avaliar a sua eficácia e eficiência, perante casos reais, confirmando ou identificando novos pontos relativos à sua operacionalização, que necessitarão de ser melhorados em face dos resultados obtidos.

[74] Os módulos de formação associados a este percurso educativo poderão resultar da reciclagem ou atualização de disciplinas já existentes, adaptando-as às necessidades mais específicas.

Bibliografia e referências

27000.org. (2008). *An Introduction to ISO 27001, ISO 27002....ISO 27008*. Obtido em 3 de novembro de 2014, de 27000.org.

Accessdata. (2015). *Forensic Tool Kit*. Obtido em 17 de janeiro de 2015, de accessdata.com: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

ACO, A. C. (2006). *Security Directive AD 70-1.* NATO.

ACQuipedia. (30 de junho de 2005). *DOTMLPF.P Analysis*. Obtido em 29 de outubro de 2014, de ACQuipedia: https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2

Anubisnetworks. (2015). *Cyberfeed*. Obtido em 17 de janeiro de 2015, de anubisnetworks.com: https://www.anubisnetworks.com/products/threat-intelligence/cyberfeed

AR, A. d. (2005). *Constituição da República Portuguesa.* Lisboa: Quid Juris? Sociedade Editora Lda.

Arraj, V. (2010). *ITIL, The Basics.*

Bardin, L. (2003). *L' analyse de contenu.* Paris: Presses Universitaires de France.

Bergamini, C. (maio/junho de 1994). Liderança: A administração do sentido. *Revista de Administração de Empresas*, pp. 102-114.

Bravo, R. e. (18 de 10 de 2014). *Geopolítica, geoestratégia e ciberespaço: Notas introdutórias.* Obtido de academia.edu: http://www.academia.edu/5543845/Geopolitica_geoestrategia_e_ciberespaco Notas_introdutorias

Calder, A., & Watkins, S. (2008). *IT Governance – A Manager's Guide to Data Security and ISO 27001/ISO 27002.* USA: Kogan Page.

CERT.PT. (18 de 1 de 2015). *Rede Nacional CSIRT - Objetivos*. Obtido de cert.pt: http://www.cert.pt/index.php/rede-nacional-csirt/objectivos

Cichonki, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide - Recomendations of the National Institute of Standards and Technology.* Special Publications 800-61.

CNCS, C. N. (2015). *Taxonomia.* Obtido de cncs.gov.pt: http://www.cncs.gov.pt/media/2015/04/Taxonomia-pt.pdf

CNSS, C. o. (2010). *National Information Assurance (IA) Glossary CNSSI Nº4009.* Obtido de ncsc.gov: http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

Cohen, F. (1984). *A Computer Virus*. Obtido em 27 de 10 de 2014, de eecs.umich.edu: http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html

Computerworld. (15 de abril de 2011). *Rede Nacional de CSIRT quer sensibilizar e cooperação com autoridades*. Obtido em 12 de abril de 2015, de computerworld.com.pt: http://www.computerworld.com.pt/2011/04/15/rede-nacional-de-csirt-quer-sensibilizar-e-cooperacao-com-autoridades

Computerworld. (12 de 05 de 2015). *Rede Nacional de CSIRT quer sensibilizar e cooperação com autoridades*. Obtido de computerworld.com.pt: http://www.computerworld.com.pt/2011/04/15/rede-nacional-de-csirt-quer-sensibilizar-e-cooperacao-com-autoridades/

Correia, M. e. (2010). *Segurança no Software.* Lisboa: FCA-Editora de Informática, Lda.

DoD, D. o. (2013). *Guidance for development and implementation of joint concepts.* Chairman of the Joint Chiefs of Staff.

DR, D. d. (1988). *SEGNAC 1 - Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, 1ª série, nº 279 3-12-1988.* Lisboa: Assembleia da República.

DR, D. d. (1990). *SEGNAC 4 - Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática, 1ª Série, nº 49 de 28-02-1990.* Lisboa: Assembleia da República.

DR, D. d. (1998). *Lei da Proteção de Dados Pessoais, 1.ª série-A, n.º 247, de 26 de Outubro de 1998, Lei n.º 67/1998.* Lisboa: Assembleia da República.

DR, D. d. (2009). *Lei do Cibercrime, Lei nº 109/2009 de 15 de Setembro.* Lisboa: Assembleia da República.

DR, D. d. (2009). *Quadro Nacional de Qualificações, DR, 1.ª série — N.º 141 — 23 de Julho de 2009 .* Lisboa: Assembleia da República.

DR, D. d. (2013). *Orientação Política para a Ciberdefesa, DR, 2.ª série — N.º 208 — 28 de outubro de 2013 .* Lisboa: Assembleia da República.

DR, D. d. (2014). *Instalação do Centro Nacional Cibersegurança, DR, 1.ª série — N.º 89 — 9 de maio de 2014 .* Lisboa: Assembleia da República.

DR, D. d. (2015). *Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015.* Lisboa: Assembleia da República.

EC, E. C. (2013). *Cybersecurity Strategy of European Union: An Open, Safe and Secure Cyberspace.* Bruxelas.

EC3, E. C. (23 de 10 de 2014). *The Internet Organized Crime Threat Assessment (IOCTA).* Obtido de EUROPOL: https://www.europol.europa.eu/sites/default/files/publications/iocta-epub.epub

E-Maps. (22 de agosto de 2013). *DOTMLPF-P.* Obtido em 03 de novembro de 2014, de e-mapsys: http://www.e-mapsys.com/DOTMLPFP(3).pdf

ENISA. (2010). *Good Pratice Guide For Incident Management.* Obtido de enisa.europa.eu: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

ENISA. (2012). *Threat Landscape - Responding to the Evolving Threat Environment.* Obtido de enisa.europa.eu: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/ENISA_Threat_Landscape/at_download/fullReport

EU, E. U. (2009). *Concept for Computer Network Operations in EU-Led Military Operations.* European Union.

Exercito. (10 de novembro de 2014). *Exercício CIBER PERSEU 14*. Obtido em 9 de maio de 2015, de exercito.pt: http://www.exercito.pt/sites/EPT/Noticias/Paginas/ExercícioCIBERPERSEU14.aspx

Gehringer, E. F. (02 de 11 de 2014). *Study Guide - What is the Slammer Worm/SQL Worm/Sapphire Worm?* Obtido de ncsu.edu: https://ethics.csc.ncsu.edu/abuse/wvt/Slammer/study.php

IDN, I. d. (2013). *Estratégia da Informação e Segurança no Ciberespaço.* Obtido de idn.gov.pt: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

IETF. (06 de 1998). *Expectations for Computer Security Incident Response - RFC 2350.* Obtido em 21 de 05 de 2015, de ietf.org: https://www.ietf.org/rfc/rfc2350.txt

ISO/IEC. (2005). *ISO 27002 - Information technology - Security techniques - Code of practice for information security management.* ISO/IEC.

ISO/IEC. (2011). *ISO 27035 - Information technology - Security techniques - Information security incident management.* ISO/IEC.

ISO/IEC. (1 de setembro de 2011). *ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management*. Obtido de iso.org: http://www.iso.org/iso/catalogue_detail?csnumber=44379

ISO/IEC. (2011). *ISO/IEC 27035:2011(en)*. Obtido em 2014, de iso.org: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en

ISO/IEC. (2013). *ISO 27001 - Tecnologia de informação, Técnicas de segurança, Sistemas de gestão de segurança da informação – Requisitos.* Lisboa: Instituto Português da Qualidade.

JANET. (s.d.). *RTIR incident handling work-flow.* Obtido em 17 de janeiro de 2015, de bestpractical.com: https://www.bestpractical.com/static/rtir/janet-workflow.pdf

Killcrece, G., & Ruefle, R. (2008). *Creating and Managing Computer Incident Response Capability (CSIRTs).* Pittsburg: Carnegie Mellon University.

Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs).* Pittsburg: Carnegie Mellon.

Langner, R. (2013). *To kill a centrifudge.* Obtido em 2 de novembro de 2014, de langner.com: http://www.langner.com/en/wp-content /uploads/2013/11/To-kill-a-centrifuge.pdf

Lenon, M. (29 de maio de 2014). *Iranian Hackers Targeted US Officials in Elaborate Social Media Attack Operation.* Obtido em 2 de novembro de 2014, de securityweek.com: http://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Mitnik, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis: Wiley Publishing.

MNCD2, M. C. (15 de abril de 2015). *MN CD2 nations expand cyber defence coordination system functionalities*. Obtido em 17 de maio de 2015, de ncia.nato.int: https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-07.aspx

NATO. (2002). *NATO COMPUTER INCIDENT RESPONSE CAPABILITY (AC/322-D/0056).* NC3B.

NATO. (2002). *NCIRC - CONCEPT OF OPERATIONS (AC/322-N/0797).* NC3B.

NATO. (2009). *Policy for NATO concept development and experimentation MC 0583.* NATO.

NATO. (2010). *NATO Concept Development and Experimentation (CD&E) Process MCM-0056/2010.* NATO.

NATO. (2011). *NATO Computer Incident Response Capability - FOC.* NATO.

NATO. (13 de março de 2013). *NATO Rapid Reaction Team to fight cyber attack*. Obtido em 14 de janeiro de 2014, de nato.int: http://www.nato.int/cps/en/natolive/news_85161.htm

NATO. (2014). *AAP-6 NATO Glossary of Terms and Definitions.* NATO.

NATO. (2014). *CC14 Training Objectives.* NCIA.

NATO. (18 de novembro de 2014). *Largest ever NATO cyber defence exercise gets underway*. Obtido em 17 de janeiro de 2015, de nato.int: http://www.nato.int/cps/es/natohq/news_114902.htm

NATO. (2014). NATO Cyber Defence Taxonomy and Definitions. Norfolk: Consultation, Command and Control Board (C3B).

NATO. (09 de 11 de 2014). *Tratado do Atlântico Norte*. Obtido de fd.uc.pt: http://www.fd.uc.pt/CI/CEE/OI/NATO/Tratado_NATO.htm

NATO. (13 de 10 de 2014). *Wales Summit Declaration.* Obtido de nato.int: http://www.nato.int/cps/en/natohq/official_texts _112964.htm

NATO. (11 de 1 de 2015). *NATO Organization*. Obtido de nato.int: http://www.nato.int/cps/en/natohq/structure.htm#OA

NCIA. (2015). *Malware Information Sharing Plataform (MISP).* Obtido em 17 de maio de 2015, de ncia.nato.int:

https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf

NCSC, N. C. (2014). *Cyber Security Assessment Nethrleands CSAN-4.* Obtido de nctv.nl: https://english.nctv.nl/Images/cybersecurityassessmentnetherlands2014_tcm92-580598.pdf?cp=92&cs=65035

NICCSN, N. I. (2015). *A Glossary of Common Cybersecurity Terminology* . Obtido de niccs.us-cert.gov: http://niccs.us-cert.gov/glossary

NIST. (24 de dezembro de 2008). *NIST General Information*. Obtido em 12 de dezembro de 2014, de nist.gov: http://www.nist.gov/public_affairs/general_information.cfm

NIST. (2015). *Special Publications (800 Series) - Computer Security.* Obtido de csrc.nist.gov: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

NIST, N. I. (4 de 2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* Obtido de nvlpubs.nist.gov: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

OGC, O. o. (2007). *ITIL3 Service Operation.* The Stationary Office.

Paquette, J. (2010). *A history of Viruses*. Obtido em 01 de maio de 2014, de Symantec.com: http://www.symantec.com/connect/articles/ history-viruses

Proposta de Estratégia Nacional de Cibersegurança. (9 de 11 de 2014). Obtido de gns.gov.pt: http://www.gns.gov.pt/media /1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf

Quivy, R., & Campenhoudt, L. (1998). *Manual de investigação em ciências sociais.* Lisboa: Gradiva.

RCTS. (2015). *Serviço de Resposta a Incidentes de Segurança da RCTS - objetivos*. Obtido em 18 de janeiro de 2015, de cert.rcts.pt: http://www.cert.rcts.pt/index.php/rede-nacional-csirt/objectivos

RCTS, R. C. (19 de 04 de 2015). *Política de classificação de incidentes da Rede.* Obtido em 19 de abril de 2015, de cert.rcts.pt: http://www.cert.rcts.pt/images/docs/Taxonomiav2.5.pdf

SANS. (24 de outubro de 2012). *Cyber Security Awareness Month - Day 24 - A Standard for Information Security Incident Management - ISO 27035*. Obtido em 5 de dezembro de 2014, de isc.sans.edu: https://isc.sans.edu/diary/Cyber+Security+Awareness+Month+-+Day+24+-+A+Standard+for+Information+%20Security+Incident+Management+-+ISO+27035/14371

SANS. (2015). *Glossary of Security Terms*. Obtido de sans.org: http://www.sans.org/security-resources/glossary-of-terms/

Strickland, J. (2008). *10 Worst Computer Viruses of All Time*. Obtido em 31 de outubro de 2014, de howstuffworks.com: http://computer. howstuffworks.com /worst-computer-viruses.htm#page=0

Symantec. (02 de 11 de 2014). *Complex Cyber Espionage Malware Discovered: Meet W32.Gauss*. Obtido de Symantec.com: http://www.symantec.com/connect/blogs/complex-cyber-espionage-malware-discovered-meet-w32gauss

Symantec. (02 de 11 de 2014). *W32.DuQu The Percursor of Next Stuxnet*. Obtido de Symantec.com: http://www.symantec.com /connect/ w32_duqu_precursor_next_stuxnet

Symantec. (1 de 11 de 2014). *W97M.Melissa.A*. Obtido de symantec.com: http://www.symantec.com/security_response/writeup.jsp?docid=2000-122113-1425-99&tabid=2

Taruu. (2009). *ITIL V3 Foundation Study guide version 4.2.2.5.* Obtido de Unideb.hu: http://www.inf.unideb.hu/~fazekasg/oktatas/ITIL_V3_Study_Guide.pdf

USArmy. (2010). *TRADOC Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan .* Obtido de Fas.org: https://fas.org/irp/doddir/army/pam525-7-8.pdf

US-CERT. (1 de 0utubro de 2014). Obtido em 12 de dezembro de 2014, de https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

Wikipedia. (2014). *GPL*. Obtido em 18 de abril de 2015, de wikipedia.org: http://pt.wikipedia.org/wiki/GPL

Wikipedia. (s.d.). *William Gibson*. Obtido em 10 de 2014, de wikipedia.org: http://en.wikipedia.org/wiki/William_Gibson

Anexos

Anexo A – Guião da entrevista escrita

Esta entrevista enquadra-se numa investigação no âmbito de uma tese de mestrado em Segurança da Informação e Direito no Ciberespaço, realizado numa parceria entre a Escola Naval, a Faculdade de Direito de Lisboa e o Instituto Superior Técnico. Os resultados obtidos apenas serão utilizados para fins académicos relacionados com a presente tese. Pretende-se que as respostas apresentadas traduzam a sua visão sobre o assunto da Capacidade de Resposta a Incidentes de Segurança da Informação no Ciberespaço. Agradecemos a sua colaboração, **muito obrigado!**

A NATO adotou uma metodologia para a implementação de novas capacidades operacionais, baseada num modelo desenvolvido pelo Departamento de Defesa Norte Americano, que pretende identificar vulnerabilidades na operacionalização de uma capacidade. O modelo avalia uma capacidade segundo várias dimensões diferentes, a saber, Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade.

Tendo em mente a operacionalização de uma Capacidade de Resposta a Incidentes de Segurança da Informação pretende-se saber a sua opinião sobre os fatores que considera fundamentais (críticos) em cada uma das diferentes dimensões.

1 – Doutrina. Esta dimensão surge relacionada com os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum.

2 – Organização. Esta dimensão diz respeito ao modo como constituir os indivíduos em equipas, e estas em unidades operacionais, para a execução de forma coordenada das funções que lhes são determinadas para atingirem os objetivos operacionais da organização.

3 – Treino. Esta dimensão está relacionada com a preparação dos diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais de resposta aos incidentes. Uma das formas de executar as ações de treino é através de exercícios sendo relevante as lições aprendidas através do treino para o aperfeiçoamento das capacidades operacionais.

4 – Material. Esta dimensão abrange basicamente a tudo o que é necessário para suportar e equipar as unidades operacionais desde os equipamentos, a tecnologia, as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão.

5 – Liderança. Esta dimensão aparece diretamente ligada preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão.

6 – Pessoal. O fator humano é determinante, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão.

7 – Infraestruturas. Esta dimensão está ligada com a disponibilização de instalações adequadas à preparação e condução das operações. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, centros de dados, distribuição de energia elétrica, controlo ambiental e outros.

8 – Interoperabilidade. Esta dimensão refere-se à necessidade de interagir com parceiros externos, através da definição de procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo.

Obrigado pela colaboração!

Anexo B – Transcrição da entrevista do eng. Lino Santos (CNCS)

O eng. Lino Santos desempenha atualmente as funções de Coordenador do Departamento de Operações e Segurança do Centro Nacional de Cibersegurança.

O texto que se segue transcreve as opiniões do eng. Lino Santos sobre o tema, expressas nas respostas disponibilizadas por escrito conforme o guião previamente apresentado no Anexo A.

1 – Doutrina. Esta dimensão surge relacionada com os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum.

Caro Comandante Baptista das Neves, gostaria de começar por enaltecer a pertinência e a importância deste tipo de trabalho, académico mas com um forte vinco prático e utilitário. Não tenho dúvidas que o resultado será de grande utilidade para a comunidade e para a Defesa em particular. Como nota prévia e de forma a enquadrar as minhas posições, faço notar que respondo a título individual e tendo como pano de fundo uma pretensa capacidade de resposta a incidentes (CSIRT), que tanto pode existir numa empresa privada como no Estado e, dentro deste, num organismo civil ou militar. Este CSIRT responde a incidentes de todo o tipo dentro de um ambiente *multistakeholder* e global (com outros CSIRT públicos e privados, empresas de cibersegurança, operadores privados de infra-estruturas e autoridades civis e militares para a cibersegurança, etc.). Deixo assim margem de manobra para o Comandante fazer a sua análise e adaptação ao contexto que lhe aprouver.

O primeiro passo para a criação de uma capacidade de resposta a incidentes passa pela construção de uma visão. Nesta devem estar claros: (1) uma definição clara da missão (objectivos estratégicos e a sua decomposição em objectivos operacionais); (2) uma definição do âmbito pessoal (constituency); (3) uma definição do âmbito material (portfólio de serviços); e (4) um conjunto de políticas que enformam a sua actuação.

Esta visão deve resultar de uma necessidade ou, por outras palavras, a probabilidade de sucesso da construção de um CSIRT é muito maior quando surge de uma necessidade reconhecida por todos, e não de um capricho individual/grupal ou de uma moda. O sucesso no estabelecimento de um CSIRT depende do grau de consciência da organização para com as ameaças e os riscos de não ter um CSIRT.

Estas quatro componentes constituem o que podemos, metaforicamente, designar de bilhete de identidade ou carta de apresentação do CSIRT e representa aquilo que somos perante a comunidade. A publicitação das mesmas revela-se de grande importância quer para a relação com a comunidade servida (âmbito pessoal), quer no contexto da cooperação com entidades externas, já que estabelecem as expectativas operacionais sobre o nosso CSIRT e constituem uma base para a necessária geração de confiança.

Respondendo agora directamente à pergunta, identifico 3 factores críticos:

(1) a clareza na definição de cada um destes elementos e a simplicidade da relação entre eles é um factor essencial de sucesso para a construção da nossa capacidade de resposta a incidentes. No fundo, os membros CSIRT, a comunidade servida e os *stakeholders* têm que perceber muito bem o papel e os limites de actuação e precisam de se sentir parte de uma máquina maior. O contexto de actuação pode exigir a definição de conceitos básicos como ciberdefesa, cibersegurança ou cibercrime para uma melhor definição de missão. Alguns exemplos concretos, com os quais já me deparei, são a definição de missão de forma muito abstrata e, por vezes, "megalómana", um portfólio de serviços que não corresponde à missão, a inclusão na comunidade constituinte de pessoas/entidades sobre as quais não se consegue exercer nenhum tipo de autoridade, a saber, total ou partilhada ou, ainda, a ausência de mecanismos de governance tais como a falta de suporte de outras unidades internas da organização ou a deficiente colocação do CSIRT dentro do organigrama da organização (eg. dentro do departamento de IT).

(2) outro factor crítico prende-se precisamente com a articulação do CSIRT com outras unidades internas à organização. Por um lado existe um forte dependência da parte do CSIRT no departamento jurídico da organização para a validação dos procedimentos operacionais e no apoio *in-loco* na gestão de situações mais complexas. Por outro, para produção de medidas (o negócio do CSIRT) é fundamental conhecer os detalhes técnicos e operacionais dos produtos/serviços para os quais se está a fazer resposta a incidentes. Em organizações de maior dimensão ou quando o CSIRT não está devidamente colocado no organigrama, isto pode ser um constrangimento à eficácia.

(2) finalmente, é importante ter definidos princípios de colaboração com entidades externas nacionais e internacionais. Nestas incluem-se a comunicação social, os *stakeholders*, ou se aplicável, a comunidade servida. O cuidado e a eficácia das comunicações com exterior são o indicador que define a reputação e subsequentemente a confiança que estas entidades externas depositam no CSIRT. Considerando que grande parte dos incidentes de cibersegurança não se circunscrevem ao âmbito de actuação de um só CSIRT, por conseguinte esse CSIRT vai precisar da ajuda da comunidade nacional e internacional de cibersegurança. É natural que essa ajuda seja tão mais rápida e eficaz quanto a confiança e reputação que o nosso CSIRT tem. Neste capítulo são importantes as políticas de *non-disclosure* que salvaguardem a identidade de vítimas, ou princípios com o *need-to-know* que enquadrem o CSIRT numa comunidade alargada.

2 – Organização. Esta dimensão diz respeito ao modo como constituir os indivíduos em equipas, e estas em unidades operacionais, para a execução de forma coordenada das funções que lhes são determinadas para atingirem os objetivos operacionais da organização.

Como bem formulado na pergunta, isso depende claramente da missão, mas principalmente do portefólio de serviços. Como pano de fundo devemos ter sempre em consideração um conjunto de princípios básicos: (1) os incidentes ocorrem em sistemas e redes de comunicações que têm um ou

mais responsáveis pela sua gestão e operação; (2) por norma, estes sistemas e redes são instrumentais e servem um qualquer “negócio” que por sua vez também tem um ou mais responsáveis; (3) as falhas e os respectivos impactos quase nunca são circunscritos a uma destas áreas funcionais ou de “negócio”.

Ou seja, é precisamos, por um lado, do *expertise* de cada uma destas áreas, acrescentando-lhe coordenação e visão agregada, e, por outro, precisamos, muitas vezes, da cobertura institucional para realizar essa coordenação com sucesso.

Posto isto, os factores críticos para a organização do CSIRT são o seu posicionamento dentro do organigrama da organização de forma a garantir quer a independência, quer a autoridade na coordenação. A titulo de exemplo, mais uma vez baseando-me na experiência, os CSIRT colocados dentro do IT, raramente conseguem ter uma avaliação plena dos incidentes que estão a tratar, preocupando-se mais em “tapar os buracos” (com os instrumentos que têm) do que identificar as fonte de problemas e medidas não tecnológicas. Isto requer que o CSIRT esteja colocado dentro organização fora das áreas áreas funcionais, reportando directamente à direcção ou à administração.

A teoria refere para além deste modelo organizacional o “CSIRT distribuído” e o “CSIRT embebido”. O primeiro quando a organização tem pólos ou campus geograficamente distantes com autonomia de gestão em cada um deles e o segundo quando a organização é suficientemente pequena que n\ao justifique uma equipa autónoma para esta função.

Outras áreas importantes que devem apoiar ou estar coordenadas com o CSIRT são o departamento jurídico que deve validar todos os procedimentos e políticas, bem como dar o apoio necessário durante as situações novas ou não tipificadas, e o departamento de comunicação/relações públicas para a gestão de situações mais complicadas do ponto de vista de imagem da organização.

É importante distinguir entre função de resposta a incidentes e operações de segurança. A criação da primeira não deve melindrar/tocar as responsabilidades previstas para a segunda.

3 – Treino. Esta dimensão está relacionada com a preparação dos diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais de resposta aos incidentes. Uma das formas de executar as ações de treino é através de exercícios sendo relevante as lições aprendidas através do treino para o aperfeiçoamento das capacidades operacionais.

O primeiro aspecto aqui a referir é a necessidade de identificar as valências técnicas e humanas necessárias para cada uma das funções. E isto depende obviamente dos serviços/produtos que são objecto do nosso CSIRT, bem como das componentes tecnológicas que lhes servem de suporte. Depois de definidas estas competências é necessário identificar ou contratar as pessoas necessárias, identificar o *gap* e desenhar um programa de formação específico para cada um.

Sobre a identificação/contratação de elementos, é importante identificar-lhe um conjunto de bases essenciais e vontade de aprendizagem. Sem as bases, a velocidade de progressão é baixa; sem a vontade de aprender, a progressão é nula.

Sobre o programa de formação é preciso ter em atenção dois tipos de risco: (1) à medida que o elemento do CSIRT vai ganhando competências, vai aumentando o risco de este vir a ser contratado por terceiros, ou seja, é preciso contratualizar fidelidade à medida que se vai dando formação; (2) o quadro de ameaças e o seu *modus operandi* está em constante mutação, pelo que o programa de formação deve ser revisto periodicamente (eg. anualmente). Um plano de formação deve ter um horizonte de 2 a 4 anos. Mais uma vez é preciso ter cuidado com a oferta que é muito distinta quanto à qualidade.

Uma boa solução é fazer crescer o portfólio de serviços à medida que se vai ganhando capacidade e competências. É uma boa forma de assegurar boa reputação.

4 – Material. Esta dimensão abrange basicamente a tudo o que é necessário para suportar e equipar as unidades operacionais desde os equipamentos, a tecnologia, as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão.

Mais uma vez, isto depende do portfólio de serviços. Se pensar-mos apenas na resposta a incidentes, os requisitos são muito poucos e existem muito boas soluções em regime de *open source*: Um sistema para registo de actividade (gestão de ocorrências); mecanismos de cifra para comunicação quer com a comunidade servida, quer com a comunidade de segurança e outros *stakeholders*; meios de comunicação para receber notificações e interagir com *stakeholders* (por norma e-mail dedicado e sem filtragem e telefone), bem como meios de divulgação de informação de alerta (o ideal é encontrar canais já existentes para este efeito); se pretendermos que o nosso CSIRT realize recolha de prova, precisamos de instrumentos específicos para o fazer em segurança; ferramentas para análise de tráfego capturado (eg. wireshark); ferramentas para análise de artefactos (eg. FTK); ou ferramentas para análise de malware (eg. cuckoo sandbox).

A opção por ferramentas pagas deve ser tomada depois de esgotar a utilização de ferramentas open source. Por um lado estas últimas podem ser usadas como um bom laboratório de treino, pois requerem uma maior interação e melhor conhecimento técnico. Por outro são a base para quase todas as ferramentas pagas que apenas acrescentam uma interface gráfica.

Em suma, o factor crítico, neste ponto deve ser o de não cair na tentação de comprar múltiplos produtos sem esgotar as capacidades dos anteriores. Este risco adenssa-se quando estamos perante um contexto muito competitivo e agressivo no que se refere a soluções comerciais para esta área. A solução também passa por focar no portfólio de serviços.

5 – Liderança. Esta dimensão aparece diretamente ligada preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para

comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão.

Neste tópico, não consigo apontar factores críticos. As características naturais de um bom líder serão suficientes, tal como noutros domínios, para a gestão de um CSIRT. Apontaria apenas algumas das competências intrínsecas a esta actividade: bons conhecimentos técnicos para realizar uma boa avaliação da situação; conhecimentos básicos de direito e legislação aplicável para melhor decidir sobre medidas e garantir o princípio da proporcionalidade; carisma e respeito das restantes áreas internas, da comunidade servida e dos *stakeholders* em geral. De Facto, a reputação de um CSIRT junto dos *stakeholders* é também a reputação do seu líder. A teoria sobre a edificação de um CSIRT indica claramente no sentido de identificar um líder capaz de gerar a confiança dentro e fora da equipa.

Posto isto, e como vem referido na pergunta, este líder deve ser capaz de tirar o melhor de cada um dos técnicos que compõem o CSIRT, proporcionando-lhes a liberdade para aprenderem e especializarem numa das áreas de competência necessárias.

6 – Pessoal. O fator humano é determinante, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão.

Já foi respondido atrás. É no entanto o factor mais crítico de todos os que são tratados aqui.

Em suma: identificar as competências técnicas e humanas, identificar as melhores pessoas, avaliar o gap e proporcionar treino.

7 – Infraestruturas. Esta dimensão está ligada com a disponibilização de instalações adequadas à preparação e condução das operações. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, centros de dados, distribuição de energia elétrica, controlo ambiental e outros.

Devem ser acauteladas as condições de segurança física, mas também lógica para tratar informação no mínimo sensível. Deve ser dada atenção especial à segurança das bases de dados de incidentes, bem como de provas recolhidas para efeito de admissibilidade em tribunal.

8 – Interoperabilidade. Esta dimensão refere-se à necessidade de interagir com parceiros externos, através da definição de procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo.

Neste ponto existem alguns standards que podem/devem ser considerados. Um diz respeito à partilha de informação (de uma forma genérica). O principal standard é o STIX e encontram-se ainda

numa fase embrionária. Existem muito poucas implementações deste modelo. A comunidade está a aderir de forma muito suave a este standard, começando primeiro por compatibilizar interfaces de entrada e saída. Este standard é importante se precisarmos de criar mecanismos automáticos de tratamento de informação trocada. Outro standard importante é o IODEF para partilha de informação sobre incidentes (ou seja sem tratamento automático). Este standard ou uma boa parte dele foi adoptada pela rede de CSIRTs para facilitar o envio/recepção de informação.

Outro aspecto diz respeito à definição de expectativas quanto ao nível/capacidade operacional de uma outra equipa de CSIRT. Aqui, os Operational Level Agreements assumem particular importância. Num contexto controlado (por exemplo a comunidade de CSIRT nacional) podemos definir que tipo de actuação temos relativamente às situações mais comuns e partilhar esse procedimento com as restantes equipas. Desta forma, se o meu CSIRT precisar da tomada de acção de outro CSIRT nacional, sei com o que posso e como contar. Este trabalho também está a ser definido dentro da rede nacional de CSIRT.

Igualmente relevante (aqui para o contexto militar) o tipo de classificação de informação relativa a eventos ou incidentes de segurança. É preciso ter em atenção que a resposta a incidentes só se faz coordenando com outras entidades públicas e privadas, nacionais e internacionais. Nenhum CSIRT actua sem ter uma evidência que realmente há algo de errado dentro da sua esfera de actuação. Ou seja, se precisarmos, por exemplo, que um operador de telecomunicações aplique alguma medida de mitigação dentro da sua rede, precisamos de dar alguma evidência de que o ataque é proveniente da sua rede.

Por último volto a referir que a confiança/reputação numa equipa de CSIRT são fundamentais para a partilha de informação e para a qualidade da cooperação no quadro da resposta a incidentes.

Anexo C – Transcrição da entrevista do eng. Gustavo Neves (RCTS ex-CERT.PT)

O eng. Gustavo Neves desempenha atualmente as funções de Gestor de Serviços de Segurança na FCT-FCCN[75].

O texto que se segue transcreve as opiniões do eng. Gustavo Neves sobre o tema, expressas nas respostas disponibilizadas por escrito conforme o guião previamente apresentado no Anexo A.

1 – Doutrina. Esta dimensão surge relacionada com os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum.

A doutrina assume um papel de relevo, na medida em que a resposta a incidentes tem implicações, filosofia e enquadramento diferentes da mais "tradicional" vertente da segurança preventiva. A resposta a incidentes pressupõe o estabelecimento de redes de confiança, obediência a boas práticas acreditadas em comunidades internacionais, e uma cultura de segurança baseada nos princípios da cooperação, não só com entidades congéneres aos CERTs, mas também com outras, tais como operadores de telecomunicações, forças policiais, comunicação social, operadores de infra-estruturas críticas e outros, dependendo do próprio âmbito de atuação ("constituency") do CERT em causa.

2 – Organização. Esta dimensão diz respeito ao modo como constituir os indivíduos em equipas, e estas em unidades operacionais, para a execução de forma coordenada das funções que lhes são determinadas para atingirem os objetivos operacionais da organização.

A dimensão organizacional está intimamente ligada ao portfólio de serviços prestados pelo CSIRT e, consequentemente, também ao tipo de âmbito de atuação ("constituency"). É essencial haver uma adequação das equipas às funções críticas que desempenha, seja na resposta a incidentes, coordenação, produção de alertas, análise forense, auditorias de segurança, etc. As competências e definições de níveis de serviço dentro da equipa deverão ser adequadas às atribuições do CERT em causa. A organização de um CERT militar, por exemplo, dará provavelmente ênfase a capacidades de ciber-defesa (compreendida como uma capacidade para um contra-ataque, o que pressupõe competências de segurança "agressiva"), ao passo que um CERT civil académico poderá pôr ênfase na proteção dos ativos de IT das instituições e na mitigação de ataques que afetem a disponibilidade do serviço de conetividade.

3 – Treino. Esta dimensão está relacionada com a preparação dos diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais de resposta aos incidentes. Uma das formas de executar as ações de treino é através de exercícios sendo relevante as lições aprendidas através do treino para o aperfeiçoamento das capacidades operacionais.

[75] FCT-FCCN – Fundação para a Ciência e Tecnologia – Fundação para a Computação Científica Nacional

O treino é essencial para manter uma capacidade de resposta efetiva a vários níveis. Se, por um lado, a experiência dita que, em tempo de emergência, pouco ou nada se passa de acordo com os planos, é também justo dizer que o treino contribui para que a preparação das equipas lhes dê vantagens quando é necessário superar o inesperado e encontrar formas novas, por vezes improvisadas, de ultrapassar a adversidade. Mas mesmo no quadro do cumprimento de um plano de emergência, é fundamental que estes sejam regularmente testados à luz do quadro de ameaças mais corrente, para verificação da sua contínua adequação. Também nesta vertente, a condução de exercícios regulares é fundamental, seja para testar a capacidade técnica a vários níveis, quer a coordenação inter-departamental, inter-agência e internacional.

4 – Material. Esta dimensão abrange basicamente a tudo o que é necessário para suportar e equipar as unidades operacionais desde os equipamentos, a tecnologia, as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão.

Sem dúvida importante, mas talvez o menos crítico de todos, na perspetiva de que é relativamente "fácil" de obter, contanto que os requisitos sejam definidos de forma competente e que haja recursos para os adquirir, manter e operar. Dependendo do portfólio de serviços de um CERT, os materiais podem ser relativamente baratos, havendo frequentemente opções gratuitas e open-source desenvolvidas dentro da própria comunidade de segurança.

5 – Liderança. Esta dimensão aparece diretamente ligada à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão.

Em qualquer tipo de organização, a capacidade de liderança é importante. É especialmente importante no sucesso de equipas de resposta a incidentes onde os recursos materiais são escassos, ou os recursos humanos carecem de motivação, ou em que os riscos resultantes da atuação do CERT são, percetivelmente, altos. São situações em que a capacidade de liderança pode contribuir para suprir carências de performance, motivação ou resultantes de receio ou pressão. De um modo geral, num universo que evolui de forma rápida e fluida, é essencial a visão de um líder que consiga adaptar continuamente a sua equipa às sempre crescentes e diferentes exigências desta atividade.

6 – Pessoal. O fator humano é determinante, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão.

Como já foi dito, a atividade de um CERT pressupõe competências especiais. É essencial a capacidade para identificar as caraterísticas únicas necessárias ao bom desempenho de funções dentro destas equipas durante a fase de recrutamento. É crucial não só identificar competências técnicas, mas também, por exemplo, identificar eventuais vulnerabilidades de personalidade que

possam redundar em divulgação (intencional ou acidental) de informação confidencial, falhas de comunicação, ou dificuldades de trabalhar em equipa ou lidar com as pressões ligadas a situações de emergência. Qualquer destas situações pode deitar a perder a eficácia no tratamento de uma situação de emergência, e/ou comprometer em minutos relações de confiança que levam anos a estabelecer.

7 – Infraestruturas. Esta dimensão está ligada com a disponibilização de instalações adequadas à preparação e condução das operações. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, centros de dados, distribuição de energia elétrica, controlo ambiental e outros.

É obviamente necessário dispor de instalações adequadas, mas talvez também seja um requisito secundário, mais uma vez na perspetiva da dificuldade de obtenção. De um modo geral, os requisitos não ditarão a necessidade de instalações com caraterísticas demasiado particulares e/ou dispendiosas, embora possa haver exceções, também elas decorrentes do tipo de âmbito de atuação e serviços prestados.

8 – Interoperabilidade. Esta dimensão refere-se à necessidade de interagir com parceiros externos, através da definição de procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo.

Absolutamente fundamental. Há, sobretudo, dois eixos essenciais que quase todos os CERTs necessitam de ter em atenção – a eficácia na resposta a incidentes e a agilização de processamento de informação sobre eventos de segurança (este último muito ligado à capacidade de automação). Relativamente ao primeiro, para resolver e mitigar um compromisso de segurança, tanto mais uma situação que esteja a causar impacto significativo, é essencial ter canais de confiança ágeis estabelecidos com todo o tipo de parceiros, dentro e fora da organização, frequentemente dentro e fora do país. É crítico aderir a standards e boas práticas de procedimentos que fomentem a confiança e a obtenção de resultados atempados. Relativamente ao processamento de eventos, qualquer CERT procura ter capacidade de “intelligence” que dê algum nível de “early warning” para ameaças emergentes, bem como de co-relacionamento com incidentes em curso. Para um processamento eficaz e eficiente deste tipo de informação, frequentemente muito volumosa e heterogénea em termos de qualidade e estrutura, a automação é necessária e, consequentemente, a interoperabilidade, no que toca a estruturação da informação trocada, bem como aos protocolos utilizados para o efeito, assume um papel determinante.

Anexo D – Transcrição da entrevista do eng. Santos Coelho (CDD)

O eng. Santos Coelho desempenha atualmente as funções de Diretor de Serviços do Centro de Dados da Defesa (CDD)

O texto que se segue transcreve as opiniões do eng. Santos Coelho sobre o tema, expressas nas respostas disponibilizadas por escrito conforme o guião previamente apresentado no Anexo A.

1 – Doutrina. Esta dimensão surge relacionada com os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum.

A "(…) utilização coordenada dos diversos meios para atingir um objetivo comum" é um enorme desafio face à complexidade do meio, a relativa juventude do tema, com impacto na experiência organizacional acumulada, e nas idiossincrasias culturais em momento de estruturação e organização de competências. É esta a dimensão onde são formuladas as políticas, normas e procedimentos e que, portanto, dão coerência a toda capacidade. O fator crítico para esta dimensão é o estabelecimento de uma visão que seja acionável e partilhada por todos os intervenientes. Não será possível edificar uma capacidade caso existam entendimentos diferentes sobre o objetivo a atingir, ainda que formulado em termos genéricos, ou quando são adotados posicionamentos irredutíveis, e por vezes falaciosos, sobre determinadas dimensões da segurança, como seja a privacidade e a necessidade de se dispor de informação para se atuar. A visão deverá moldar uma abordagem de compromissos aos diferentes pares antagónicos de temas que irão inevitavelmente surgir.

2 – Organização. Esta dimensão diz respeito ao modo como constituir os indivíduos em equipas, e estas em unidades operacionais, para a execução de forma coordenada das funções que lhes são determinadas para atingirem os objetivos operacionais da organização.

Entendendo esta dimensão a um nível mais operacional, considera-se que, comparativamente com a anterior, será mais simples de alcançar. Os aspetos mais críticos desta dimensão são o de organizar equipas que reúnam as diferentes competências, que utilizem um vocabulário que todos compreendam, de modo a maximizar a exploração das diferentes competências num determinado caso concreto.

3 – Treino. Esta dimensão está relacionada com a preparação dos diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais de resposta aos incidentes. Uma das formas de executar as ações de treino é através de exercícios sendo relevante as lições aprendidas através do treino para o aperfeiçoamento das capacidades operacionais.

A execução de ações de treino, mais ou menos elaboradas, será também um aspeto comparativamente menos difícil. No entanto, a questão mais crítica nesta dimensão é a de formalizar a ligação dos exercícios ao ciclo de vida da gestão do conhecimento na organização através de instrumentos como a identificação de lições que deverão, posteriormente, passar a aprendidas.

4 – Material. Esta dimensão abrange basicamente a tudo o que é necessário para suportar e equipar as unidades operacionais desde os equipamentos, a tecnologia, as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão.

Sendo esta a dimensão mais tecnológica, o aspeto mais crítico desta dimensão é o de ser (erradamente) privilegiada uma abordagem que dê primazia à operação tática de uma determinada ferramenta, relegando para segundo plano os aspetos arquiteturais que, podendo ser dispensáveis em contextos mais simples, são absolutamente cruciais quando se aumenta a complexidade deste tipo de recursos. Considerando o pressuposto comummente aceite de que esta capacidade deverá enquadrar-se num ecossistema de parceiros que habilitem a visibilidade e eventual intervenção no ciberespaço de interesse, os aspetos arquiteturais das soluções assumem-me como muito relevantes.

5 – Liderança. Esta dimensão aparece diretamente ligada à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão.

As competências multidisciplinares necessárias para edificar uma equipa efetiva pode induzir a ascensão a lugares de chefia de elementos com capacidades muito boas numa determinada área, desvalorizando um aspeto que parece revelar-se como um dos mais importantes, que é o da capacidade para manter a equipa focada e estar disponível para liderar a equipa num caminho de avaliação permanente podendo, eventualmente, em determinados momentos, dar primazia a aspetos que não os da respetiva área de proveniência. Dito de outra maneira, as competências relevantes para a liderança da equipa não são exatamente as mesmas que fazem de um determinado elemento alguém muito competente numa determinada área. Assim, o fator mais relevante nesta dimensão é o discernimento para efetuar essa distinção e edificar um mapa de competências que contemple as que são necessárias para a função.

6 – Pessoal. O fator humano é determinante, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão.

Dimensão com relativa clareza naquilo que é necessário fazer, sem que isso signifique que seja trivial. O aspeto mais crítico é o balanceamento incorreto de determinadas dimensões das competências necessárias, com impacto nos resultados a alcançar pela equipa. Um aspeto a salientar é o de habitualmente não se separar as competências de cariz estritamente técnico da estrutura de comando e controlo que materializa o fluir da autoridade na cadeia de comando para efetuar uma determinada ação. Este aspeto pode vir a revelar-se bloqueador uma vez que o ciclo de vida destas capacidades não é o mesmo, com as competências tecnológicas a terem um tempo de vida útil muito mais curto.

7 – Infraestruturas. Esta dimensão está ligada com a disponibilização de instalações adequadas à preparação e condução das operações. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, centros de dados, distribuição de energia elétrica, controlo ambiental e outros.

Nesta dimensão julgo não haver grande dificuldade. As maiores dificuldades poderão resultar de entendimentos menos apropriados nas outras dimensões que depois poderão vir a ter impacto nesta.

8 – Interoperabilidade. Esta dimensão refere-se à necessidade de interagir com parceiros externos, através da definição de procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo.

Esta é uma dimensão absolutamente crucial, conforme já aludido na resposta à questão da dimensão material. Para além da normalização dos procedimentos, modelos de dados, informação estruturada, etc., (que só por si se constituem desde logo como um grande desafio) parece ser muito importante que, face à rapidez com que os acontecimentos se podem desenrolar neste domínio, é muito importante que as tecnologias também suportem a interoperabilidade de modo a habilitar atuações eficazes.

Anexo E – Taxonomia de incidentes de segurança (exemplo)

O Centro Nacional de Cibersegurança publicou uma taxonomia para classificar incidentes e eventos de segurança baseada na taxonomia da Rede Nacional de CSIRT[76].

CLASSE DE INCIDENTE	TIPO DE INCIDENTE
Código Malicioso	Malware
	Botnet Drone
	Ransomware
	Malware Configuration
	C&C
Disponibilidade	DDoS
Recolha de Informação	Scanner
Tentativa de Intrusão	Exploit
	Brute-force
	IDS alert
Intrusão	Defacement
	Compromised
	Backdoor
Segurança da Informação	Dropzone
Fraude	Phishing
Conteúdo Abusivo	SPAM
Vulnerável	Vulnerable Service
Outro	Outro

[76] http://www.cncs.gov.pt/media/2015/04/Taxonomia-pt.pdf, consultado em 19-04-2015

Anexo F – RFC 2350 Núcleo de Resposta a Incidentes de Segurança da Informação

RFC 2350 do Núcleo RISI (exemplo)

1. Informação sobre o documento

Este documento contém a descrição do Núcleo RISI de acordo com a RFC 2350. Disponibiliza informações sobre a configuração do Núcleo CRISI, os canais de comunicação disponibilizados e a sua responsabilidade.

1.1. Data da última atualização

Version 1.0 2015/05/21

1.2. Lista de distribuição

Todas as UEO da Marinha

1.3. Localização do documento

Este documento encontra-se disponibilizado na página da CRISI (crisi.marinha.pt)

1.4 Autenticação do documento

Este documento encontra-se assinado digitalmente

1.5 Identificação do documento

Titlo: " **RFC 2350 do Núcleo RISI**"

Versão: 1.0

Data: maio 2015

2. Contactos

2.1. Nome da equipa

Núcleo de Resposta a Incidentes de Segurança da Informação (NRISI)

2.2. Morada

STI – Núcleo RISI
Base Naval de Lisboa
2800 ALMADA,
Portugal

2.3. Fuso horário

UTC +00:00

2.4 Numero Telefone

+351 210 999 999

2.5 Numero Fax

351 210 999 999

2.6 Endereço eletrónico

Todos os incidentes devem ser reportados para nrisi@marinha.pt

2.9 Membros da equipa

O NRISI é liderado pelo Capitão-Tenente Paulo Ficticius. O Núcleo é constituído por elementos da STI, DITIC e COMNAV distribuídos da seguinte forma (ler nr elementos / função):
8 / Monitorização de Eventos
3 / Gestores de Incidentes
2 / Analistas Forenses

2.10 Outras informações

2.11 Métodos de contato

O método preferível de contato é via e-mail (nrisi@marinha.pt) o qual é monitorizado durante as horas normais de serviço.

Em caso de urgência contatar para o telefone +351 910 999 999, o qual é monitorizado 24 h x 7 dias

Horário normal de serviço: 08:30 to 17:30 de segunda a sexta-feira

3. Guião

3.1 Missão

A missão do NRISI é preparar, detetar, reagir e recuperar de incidentes de segurança da informação que possam ocorrer no âmbito das suas infraestruturas de informação e Comunicações da Marinha.

(O presente anexo tem apenas como objetivo exemplificar a elaboração da RFC 2350 e a sua importância na comunicação com a comunidade constituinte, não se apresentando por isso os restantes pontos da RFC 2350)

Anexo G – Workflow de resposta aos incidentes