TÉCNICO LISBOA

Gestão de Incidentes de Cibersegurança em Organizações Públicas

Daniel Matos

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática e de Computadores

Orientadores: Prof. Miguel Leitão Bignolas Mira da Silva
Eng. Nuno Miguel Brás Fernandes

Júri

Presidente: Prof. Paolo Romano
Orientador: Prof. Miguel Leitão Bignolas Mira da Silva
Vogal: Prof. José Luís Brinquete Borbinha

Outubro 2018

Agradecimentos

Dedico este trabalho à minha família, em especial à minha esposa e aos meus filhos, pelo tempo que não lhes pude dedicar, mas que foram e são a minha força e o meu suporte. Estão sempre lá. Obrigado.

Um agradecimento especial aos meus orientadores Professor Miguel Mira da Silva e ao Eng. Nuno Fernandes do Centro Nacional de Cibersegurança pelo apoio e acompanhamento dado, mesmo nos momentos difíceis, e com agendas preenchidas, tiveram sempre um momento para incentivar e orientar.

Quero agradecer a todos os que me encorajaram, incentivaram e acompanharam na realização deste trabalho.

Agradeço a todos aqueles que abdicaram de algum do seu tempo para colaborar, partilhar e contribuir com o seu conhecimento e saber.

Um obrigado aos colegas de trabalho pelo incentivo, esclarecimentos e contributos, que muito agradeço, para que esta etapa se concluísse e chegasse a bom porto.

A todos os que mencionei e não mencionei o meu muito obrigado.

Abstract

The inadequate preparation of organizations to deal with increasingly sophisticated cyberattacks is publicly recognized. The cybersecurity incidents should be managed in accordance with a process for cybersecurity incident management. Using the research methodology *Design Science*, we propose a reference process based on standards and guidelines of international good practices, with the aim of contributing to the implementation of the cybersecurity incident management process in Portuguese organizations. The proposed reference process was evaluated in practice in a public organization in Portugal.

Keywords: cibersecurity; incident management; ISO 27035; cyberattacks

Resumo

A insuficiente preparação das organizações para lidar com ciberataques cada vez mais sofisticados é reconhecida publicamente. Os incidentes de cibersegurança devem ser geridos de acordo com um processo para gestão de incidentes de cibersegurança. Utilizando a metodologia de investigação *Design Science*, propomos um processo de referência baseado em normas e guias de boas práticas internacionais, com o objetivo de contribuir para a implementação do processo de gestão de incidentes de cibersegurança nas organizações portuguesas. O processo de referência proposto foi avaliado na prática numa organização pública em Portugal.

Keywords: cibersegurança; gestão de incidentes; ISO 27035; ciberataques

Conteúdo

Lista de Figuras

Acrónimos

CEO Chief Executive Officer. 30, 33, 37

CERT Computer Emergency Response Team. 9, 20

CNCS Centro Nacional de Cibersegurança. 2, 12, 14–16, 33, 46

CSIRT Computer Security Incident Response Team. 2, 9, 10, 12, 17, 18, 43–47, 49

DS Design Science. 3, 4, 41, 54, 56

ENCS Estratégia Nacional da Segurança do Ciberespaço. 14, 32

ENISA Agência Europeia para a Segurança das Redes e da Informação. 17, 20

ISACA Associação de Auditoria e Controle de Sistemas de Informação. 19

IT Information Tecnology. 33, 37

ITIL IT Infrastructure Library. 18, 19

MAI Ministério da Administração Interna. 34

NIS Network and Information Security. 35

NIST National Institute of Standards and Technology. 21, 35

OPC Orgão de Polícia Criminal. 34

RASI Relatório Anual de Segurança Interna. 2

RNCSIRT Rede Nacional de CSIRT. 10, 17, 44

SANS SANS Institute. 19

SIM3 Security Incident Management Maturity Model. 18, 47

SRI Segurança das Redes e da Informação. 11, 12

TI Tecnologias de Informação. 3, 18–20, 34, 37

TLP Traffic Light Protocol. 17, 43, 46

UE União Europeia. 11, 20, 35

Capítulo 1

Introdução

Neste capítulo 1 enquadramos e apresentamos o problema a que pretendemos dar resposta, a metodologia de investigação utilizada para a sua resolução e a estrutura desta dissertação.

Este trabalho insere-se na área da cibersegurança. A escolha do tema Gestão de Incidentes de Cibersegurança em Organizações Públicas levou em consideração os inúmeros casos que têm vindo a público relacionados com ataques informáticos dirigidos a diferentes organizações e Estados.

As organizações públicas também estão expostas e devem ser capazes de gerir e reagir a incidentes de cibersegurança.

1.1 Problema

Segundo a Comissão Europeia [3], só em 2016, ocorreram mais de 4 000 ataques diários com recurso a software de sequestro, também designado *ransomware* [4], tendo 80% das empresas europeias sofrido pelo menos um incidente de cibersegurança. Este documento refere ainda que, só nos últimos quatro anos, o impacto económico da cibercriminalidade aumentou cinco vezes.

Um dos casos públicos e que ocorreu em 12 de maio de 2017, foi o ataque de *ransomware* que ficou conhecido como *WannaCry*[1]. Esta ameaça chega através de um anexo recebido por correio eletrónico ou de outras máquinas de uma mesma rede informática. Quando o anexo é aberto inicia-se a execução e replicação por máquinas com sistemas operativos Microsoft Windows instalados, explorando uma vulnerabilidade já conhecida e identificada pela Microsoft [5]. Depois de ter acesso ao sistema, procura cifrá-lo, e quando consegue, impede o seu normal funcionamento e apresenta uma mensagem com informações de ameaça, com a solicitação de um resgate financeiro para que seja remetida a solução para a recuperação dos dados, o que pode nem acontecer ou a informação recebida não funcionar.

Este incidente com o *WannaCry*, e de acordo com o relatório da investigação do *National Audit Office* (NAO), no Reino Unido, propagou-se por mais de 200.000 computadores e teve um impacto num curto espaço de horas em mais de 100 países. Os danos causados foram nas mais diversas áreas. Destaca a área da saúde em Inglaterra, onde o *National Health Service* (NHS) foi afetado e causou a disrupção de serviços, levando ao cancelamento e adiamento de inúmeras consultas [6].

Tendo presente o artigo publicado no SapoTek [2], é possível extrair que as ameaças à cibersegurança

[1] Consultar: https://www.symantec.com/security-center/writeup/2017-051310-3522-99; Acedido em 17-09-2018

[2] Consultar: https://tek.sapo.pt/noticias/computadores/artigos/ciberseguranca-cooperacao-entre-diferentes-entidades-e-obrigatoria-para-enfrentar-os-riscos-crescentes; Acedido em 10-09-2018

estão a crescer, os hackers estão a especializar-se e os riscos aumentam com impactos económicos cada vez maiores, (...) falhas de segurança que estão muitas vezes escondidas porque as organizações ainda não as descobriram ou revelaram que foram atacadas [7].

Ainda recentemente, no dia 04 de agosto de 2018, soube-se pelo jornal Diário de Notícias[3] que os Hospitais da CUF, pertencentes ao grupo José de Mello Saúde, em Portugal, foram alvo de um ataque informático que impediu a utilização dos computadores do grupo. O vírus informático que terá infetado os sistemas dos hospitais tinha o nome de SamSam[4] e bloqueou o acesso à informação. Devido a essa situação o acesso aos registos dos doentes foi difícil ou mesmo impossível.

Estes são alguns exemplos reais que aconteceram e que evidenciam que os ciberataques ocorrem com frequência bem como alguns dos seus efeitos.

Cada vez mais, os serviços oferecidos e prestados aos cidadãos são suportados em tecnologia e infraestruturas tecnológicas que podem estar expostas a ataques e ameaças, que os podem comprometer, e a ciberameaças que são cada vez em maior número e mais disruptivas [8], causando por inerência perturbações no quotidiano da vida das pessoas.

Observando os dados nacionais constantes no Relatório Anual de Segurança Interna (RASI) [9], referentes a 2017, e respeitantes à Cibersegurança, o *Computer Security Incident Response Team (CSIRT)* nacional CERT.PT[5], equipa de resposta a incidentes de cibersegurança do Centro Nacional de Cibersegurança (CNCS), recebeu 1.895 notificações, das quais 535 (cerca de 28%) resultaram na abertura de incidentes analisados e resolvidos com sucesso. Dos incidentes analisados e resolvidos, 17% afetaram direta ou indiretamente entidades do Estado, o que representa um acréscimo de 8% em relação a 2016.

Ainda no RASI, é mencionado que a criminalidade informática e praticada usando tecnologia verifica um aumento generalizado, comparado a 2016. Em relação ao cibercrime surgem, com índices de ocorrência muito elevados, o *ransomware*, a exfiltração de dados, a exploração de vulnerabilidades dos sistemas, contendo dados sensíveis dos utilizadores, e vulnerabilidades de equipamentos.

Do exposto, formulamos uma questão e que nos leva ao problema: Estarão as organizações públicas suficientemente preparadas para gerir incidentes de cibersegurança?

O problema da insuficiente preparação para lidar com ciberataques foi reconhecida pelo Presidente da Comissão Europeia, Jean-Claude Juncker, no dia 19 de setembro de 2017 em Bruxelas [3]. Também a nível nacional, em 30 de junho de 2017, Hélder Rosalino, administrador do Banco de Portugal, referiu que as organizações não estão suficientemente preparadas para enfrentar esta ameaça nem conscientes do que a mesma representa [10].

Perante esta realidade é premente que as organizações se preparem e capacitem para fazerem uma adequada gestão de incidentes de cibersegurança que as podem afetar. Estes devem ser geridos de acordo com um processo para gestão de incidentes de cibersegurança.

Com a realização deste trabalho propomos um processo de referência[6] baseado em normas e guias de boas práticas internacionais, com o objetivo de contribuir para a implementação do processo

[3]Consultar: https://www.dn.pt/pais/interior/hospitais-da-cuf-alvo-de-ataque-informatico-9678447.html; Acedido em 10-09-2018
[4]Consultar: https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/; Acedido em 17-09-2018
[5]Consultar: https://www.cncs.gov.pt/certpt/; Acedido em 12-12-2017
[6]Designamos processo de referência a um processo que serve de referência

de gestão de incidentes de cibersegurança nas organizações portuguesas.

1.2 Metodologia de investigação

A metodologia de investigação adotada para este trabalho é a *Design Science (DS)* [1]. O objetivo da DS é ser útil na criação e avaliação de artefactos para resolver problemas organizacionais identificados. Os artefactos podem ser construções (vocabulário e símbolos), modelos (abstrações e representações), métodos (algoritmos e práticas) e instanciações (implementações e protótipos de sistemas).

Pretendemos com esta pesquisa criar um artefacto para um problema específico. Este artefacto de Tecnologias de Informação (TI) é definido como um método. A pesquisa em DS deve seguir as seguintes diretrizes:

- **Desenhar um artefacto -** Produzir um artefacto viável na forma de uma construção, modelo, método ou instanciação para determinado problema;
- **Relevância do problema -** Desenvolver soluções baseadas em tecnologia para o problema especificado;
- **Avaliação -** A utilidade, a qualidade e a eficácia do artefacto devem ser rigorosamente demonstradas por meio de métodos de avaliação bem executados;
- **Contribuições -** Fornecer contribuições claras e verificáveis. O artefacto deve ser inovador, resolvendo um problema até então não resolvido ou resolver um problema conhecido de uma forma mais eficaz ou maneira eficiente;
- **Rigor da Pesquisa -** Aplicação de métodos rigorosos tanto na construção como na avaliação do artefacto;
- **Processo de pesquisa -** Utilização dos meios disponíveis para alcançar uma solução para o problema;
- **Comunicação da Pesquisa -** Os resultados da pesquisa devem ser apresentados de forma eficaz.

Como referência neste trabalho, seguiremos a *Information Systems Research Framework* [1], que apresenta conceptualmente, conforme a Figura 1.1, a estrutura para se entender, executar e avaliar uma investigação num Sistema de Informação.

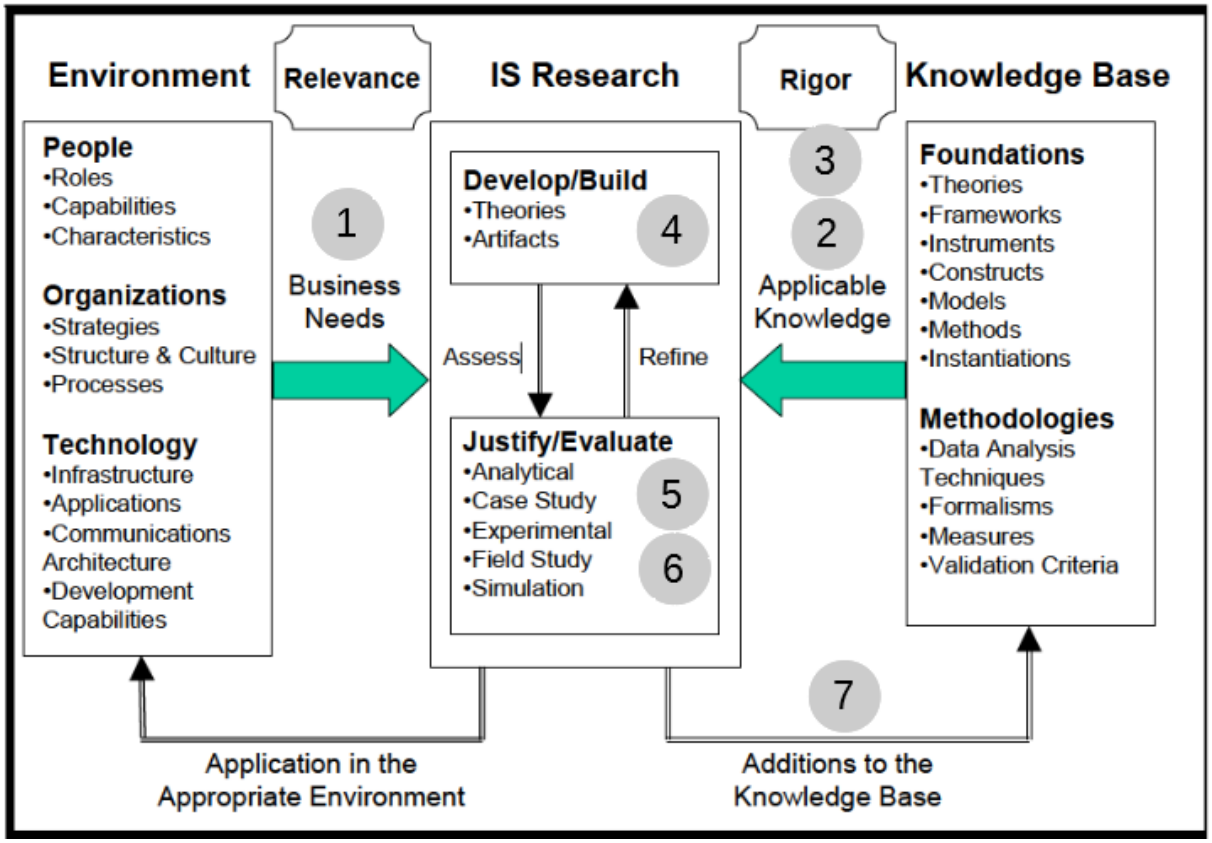

Figura 1.1: *Information Systems Research Framework* - Adaptado [1]

Descrevendo os seus componentes, o *Environment*, constituído por pessoas, organizações e tecnologias, define o espaço do problema e onde se encontra o fenómeno de interesse. Aqui estão os objetivos, tarefas, problemas e oportunidades que definem o *Business Needs*. Estando percebidos, definem-se as necessidades ou o problema e enquadrados com as atividades de pesquisa garantem a relevância da pesquisa.

A DS aborda a pesquisa, entenda-se *IS Research*, através da construção e avaliação de artefactos projetados para responder às necessidades identificadas. No momento da avaliação podem ser encontradas não conformidades no artefacto e haver a necessidade de refinar e reavaliar. Esse processo de refinamento e reavaliação é normalmente descrito em pesquisas futuras.

A *Knowledge Base* fornece as fontes de e através das quais a pesquisa é realizada e constituída por fundamentos e metodologias. Os resultados de pesquisas anteriores e de disciplinas de referência fornecem teorias, enquadramentos, instrumentos, construções, modelos, métodos e instanciações a serem usadas na fase de desenvolvimento/construção da pesquisa. As metodologias fornecem diretrizes utilizadas na fase de justificação/avaliação. O rigor atinge-se pela aplicação de fundamentos e metodologias existentes.

No final, as contribuições da pesquisa são avaliadas à medida que são aplicadas às necessidades identificadas num ambiente adequado e adicionadas ao conteúdo da *Knowledge Base* para pesquisas e práticas futuras.

Para se perceber a relação das fases da *Information Systems Research Framework* com a estrutura desta dissertação, que está organizada em sete capítulos, introduzimos na Figura 1.1 marcadores com os números de 1 a 7 e que estão mapeados com cada um dos seus capítulos.

No capítulo 1 fazemos o enquadramento, contextualização e identificação do problema e a motivação para a realização deste trabalho. Como método de investigação referimos e adotamos a metodologia *Design Science*. Seguidamente, no capítulo 2 é apresentada a revisão da literatura. No capítulo 3 apresentamos o resultado de entrevistas concretizadas a especialistas de cibersegurança. No capítulo 4 apresentamos os objetivos para uma solução. No capítulo 5 demonstramos a solução que será posteriormente avaliada. Realizamos a avaliação ao trabalho desenvolvido no capítulo 6 e, por fim, no capítulo 7 concluímos o trabalho de pesquisa e efetuamos uma análise ao trabalho realizado, apresentando contribuições, as limitações e propostas para trabalhos futuros.

Capítulo 2

Trabalho relacionado

Neste capítulo 2 analisamos o trabalho relacionado e literatura relevante sobre o tema. Detalhando, referimos um conjunto de conceitos de base relacionados, o quadro legal aplicável, normas e guias internacionais de referência no tema.

2.1 Conceitos de base

Apresentamos alguns dos conceitos base utilizados neste trabalho e a sua definição para melhor entendimento e contextualização.

No âmbito desta dissertação, e por uma questão de simplificação, designaremos incidentes de segurança da informação por incidentes de cibersegurança. Quando se fizer referência a incidentes entenda-se incidentes de cibersegurança.

Cibersegurança - conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem [11]. Precauções e ações tomadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas[12].

Ciberespaço - ambiente complexo, de valores e interesses materializando uma área de responsabilidade coletiva, que resulta da interação entre pessoas, informação, sistemas de informação, equipamentos tecnológicos e redes digitais, incluindo a Internet [11].

Risco - uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação [4].

Tratamento do Risco - atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou monitorização do risco [4].

Incidente - um evento com efeito adverso real na segurança das redes e dos sistemas de informação [13] [14]. Ações tomadas através da utilização de uma rede de computadores que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada [15].

Incidente de segurança das redes e da informação - uma ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores que resulta, ou pode resultar, na perda da confidencialidade ou integridade da informação ou prejudica o desempenho de uma rede de comunicação de dados ou sistema. Normalmente um incidente de segurança das redes e da informação significa uma violação da política de segurança de uma organização [16].

Ciberataque - ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente [4].

Cibercrime - crime previsto e punido na Lei do Cibercrime, todo o crime que recorre a tecnologia informática ou que se passa no ciberespaço [17]. Conjunto das ações ilícitas contra sistemas informáticos, mas também aquelas realizadas através dos sistemas informáticos ou cuja principal fonte de prova assume a forma digital [18].

Ciberdefesa - atividade do Estado Português destinada a garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas através do ciberespaço [11].

Norma - uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória [15].

Equipa de resposta a incidentes de segurança informática - a equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação [15].

Tratamento de incidentes - todos os procedimentos de apoio à deteção, análise e contenção de um incidente, e à resposta ao incidente [14].

Infraestrutura crítica - a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções [15].

Rede e sistema de informação - qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção [15].

Segurança das redes e dos sistemas de informação - a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles [15].

2.1.1 Administração Pública

A Administração Pública Portuguesa é uma realidade vasta e complexa [19]. Organicamente é um sistema de órgãos, serviços e agentes do Estado e de outras entidades públicas, que com o desenvolvimento das suas atividades, visam a satisfação regular e contínua das necessidades coletivas.

Compreende três grandes grupos de entidades. A administração direta do Estado que está hierarquicamente subordinada ao Governo, enquanto órgão supremo da Administração Pública; a administração indireta do Estado que está sujeita à sua superintendência e tutela; e a administração autónoma que está sujeita à sua tutela.

Quanto à competência territorial dividem-se em serviços centrais, com competência em todo o território nacional, e serviços periféricos com uma competência territorialmente limitada.

A administração indireta do Estado integra as entidades públicas, distintas da pessoa coletiva "Estado", dotadas de personalidade jurídica e autonomia administrativa e financeira que desenvolvem uma atividade administrativa que prossegue fins próprios do Estado.

A administração autónoma compreende entidades que prosseguem interesses próprios das pessoas que as constituem e que definem autonomamente e com independência a sua orientação e atividade; estas entidades agrupam-se em três categorias: Administração Regional; Administração Local e Associações Públicas. O substrato destas entidades é de natureza territorial, no caso da Administração Regional e da Administração Local, e de natureza associativa, no caso das Associações Públicas.

A Administração Regional tem a mesma matriz organizacional da administração direta e da administração indireta do Estado.

As associações públicas são pessoas coletivas de natureza associativa, criadas pelo poder público para assegurar a prossecução dos interesses não lucrativos pertencentes a um grupo de pessoas que se organizam para a sua prossecução.

2.1.2 CERT

O primeiro grande ataque de um worm[1] a nível mundial verificou-se no final da década de 1980. Foi denominado Morris[2] e disseminou-se rapidamente, tendo contaminado um grande número de sistemas informáticos. Este incidente funcionou como um sinal de alerta. As pessoas tomaram consciência de que a cooperação e a coordenação entre administradores de sistemas e gestores informáticos eram necessárias para resolver casos como este. Poucos dias após o incidente, a *Defence Advanced Research Projects Agency* (DARPA) criou a *Computer Emergency Response Team/Coordination Center* (CERT/CC), localizado na Carnegie Mellon University, em Pittsburgh, tornando-se na primeira CSIRT.

Ao longo dos anos, as *Computer Emergency Response Team (CERT)* foram alargando as suas capacidades e deixaram de ser apenas reativas, passando a fornecer outros serviços de segurança, como alertas e recomendações de segurança. Com essa evolução, o termo "CERT" depressa foi considerado insuficiente, e levou à criação do novo termo "CSIRT", no final da década de 1990. Atualmente, ambos os termos CERT e CSIRT são usados como sinónimos, sendo CSIRT o termo mais correto, segundo a

[1] Consultar: https://www.psafe.com/blog/worm/; Acedido em 20-09-2018

[2] Consultar: https://www.kaspersky.com.br/blog/caso-morris-worm-completa-25-anos/1632/; Acedido em 20-09-2018

ENISA [20].

Existem várias abreviaturas para o mesmo tipo de equipas:

- CERT ou CERT/CC - *Computer Emergency Response Team/Coordination Center* – Equipa de Resposta a Emergências Informáticas/Centro de Coordenação;
- CSIRT - *Computer Security Incident Response Team* - Equipa de Resposta a Incidentes de Segurança Informática;
- IRT - *Incident Response Team* – Equipa de Resposta a Incidentes;
- CIRT - *Computer Incident Response Team* – Equipa de Resposta a Incidentes Informáticos;
- SERT - *Security Emergency Response Team*– Equipa de Resposta a Emergências de Segurança.

Por uma questão de simplificação e normalização dos termos, neste documento, mantemos e utilizaremos o termo CSIRT para referenciar qualquer uma das equipas.

Trata-se de uma equipa de peritos de segurança informática que tem como principal atividade responder aos incidentes de segurança informática solicitados pela comunidade de utilizadores servida [20]. Dispor de uma equipa de segurança informática dedicada ajuda as organizações a atenuarem e prevenirem os incidentes, bem como a proteger os seus recursos. Outros possíveis benefícios são:

- Coordenação centralizada para as questões de segurança informática na organização.
- Gestão e resposta centralizadas e especializadas em matéria de incidentes informáticos.
- Contar com peritos disponíveis para apoiarem e ajudarem os utilizadores a recuperarem dos incidentes de segurança.
- Tratar das questões jurídicas e preservar provas em caso de ação judicial.
- Acompanhar a evolução no domínio da segurança.
- Estimular a cooperação em matéria de segurança informática no seio da comunidade utilizadora.

2.1.3 Rede Nacional de CSIRT

A Rede Nacional de CSIRT (RNCSIRT) [16] é atualmente constituída por trinta e seis entidades de diversos setores de atividade. Uma entidade para ser membro da RNCSIRT, para além de diversos requisitos, tem de possuir uma equipa de resposta a incidentes de segurança informática CSIRT formalizada e anunciada.
Os principais objetivos da RNCSIRT são:

- Estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;
- Criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contra-medidas pró-ativas e reativas;
- Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;

- Promover uma cultura de segurança em Portugal.

Disponibiliza ainda aos seus membros um conjunto de serviços tais como: serviço de diretório, workshops de segurança, coordenação de incidentes de segurança, alertas de segurança, fórum técnico e informação estatística e indicadores.

2.2 Quadro legal

O quadro legal aplicável contempla diversos diplomas relacionados com a cibersegurança. Analisamos aqueles considerados com maior relevância.

2.2.1 Diretiva SRI

A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho [14], de 6 de julho de 2016, denominada Diretiva da Segurança das Redes e da Informação (SRI), e já transposta para a legislação nacional pela Lei n.º 46/2018, de 13 de agosto [15], foi o primeiro ato legislativo horizontal da União Europeia (UE) que aborda os desafios em matéria de cibersegurança e constituiu um ponto de viragem no que respeita às capacidades de resistência e cooperação da Europa em matéria de cibersegurança.

A Diretiva SRI tem três objetivos principais [21]:

- Melhorar as capacidades nacionais em matéria de cibersegurança;
- Reforçar a cooperação a nível da UE;
- Promover uma cultura de gestão dos riscos e comunicação de incidentes entre os principais agentes económicos, nomeadamente os operadores de serviços essenciais para a manutenção de atividades económicas e sociais e os prestadores de serviços digitais.

O seu anexo II refere-se particularmente aos seguintes setores e subsetores:

- Energia: eletricidade, petróleo e gás;
- Transportes: transporte aéreo, transporte ferroviário, transporte marítimo e por vias navegáveis interiores e transporte rodoviário;
- Setor bancário: instituições de crédito;
- Infraestruturas do mercado financeiro: plataformas de negociação, contrapartes centrais;
- Saúde: prestadores de cuidados de saúde (nomeadamente hospitais e clínicas privadas);
- Água: fornecimento e distribuição de água potável;
- Infraestruturas digitais: pontos de troca de tráfego, prestadores de serviços do sistema de nomes de domínio, registos de nomes de domínio de topo.

A Diretiva SRI é uma das pedras angulares da resposta da UE às crescentes ciberameaças e desafios que acompanham a digitalização da nossa vida económica e social [21]. O seu artigo 9.º refere expressamente a segurança dos sistemas de tecnologias da informação, e impõe a adoção de medidas técnicas e organizativas específicas relacionadas com a manutenção de um quadro sólido de segurança da informação para a gestão dos riscos em matéria de segurança informática. Medidas que

devem incluir mecanismos e procedimentos que garantam a disponibilidade dos serviços, bem como a proteção da autenticidade, integridade e confidencialidade dos dados [22].

2.2.2 Centro Nacional de Cibersegurança

O Decreto-Lei n.º 136/2017 [23], de 6 de novembro, procede à terceira alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, alterado pelo Decreto-Lei n.º 162/2013, de 4 de dezembro e pelo Decreto-Lei nº. 69/2014 de 9 de maio, aprova a orgânica do Gabinete Nacional de Segurança e estabelece os termos do funcionamento do Centro Nacional de Cibersegurança.

O Centro Nacional de Cibersegurança funciona no âmbito do Gabinete Nacional de Segurança e é a Autoridade Nacional de Cibersegurança.

Tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais [15].

O "CERT.PT" funciona no Centro Nacional de Cibersegurança e é a CSIRT nacional [15].

2.2.3 Regime Jurídico de Segurança do Ciberespaço

A Diretiva SRI impunha a sua transposição para o ordenamento jurídico nacional até maio de 2018, tal já se verificou com a publicação de Lei n.º 46/2018, de 13 de agosto [15]. Esta última estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

O seu âmbito de aplicação compreende: a Administração Pública, entenda-se o Estado, as regiões autónomas, as autarquias locais, as entidades administrativas independentes, os institutos públicos, as empresas públicas e as associações públicas; os operadores de infraestruturas críticas; os operadores de serviços essenciais; os prestadores de serviços digitais e a quaisquer outras entidades que utilizem redes e sistemas de informação. De fora, ficam as redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas e as redes e sistemas de informação que processem informação classificada.

O presente regime jurídico não prejudica o cumprimento da legislação aplicável quanto à proteção de dados pessoais, designadamente o disposto no Regulamento (UE) n.º 2016/679 [24], do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), e na Lei n.º 26/2016 [25], de 22 de agosto.

Os operadores de serviços essenciais enquadram-se num dos tipos de entidades que atuam nos setores e subsetores, conforme mostrado na Figura 2.1.

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais

Setor	Subsetor	Tipo de entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.
Transportes	Transporte aéreo	Transportadoras aéreas. Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos. Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
	Transporte ferroviário	Gestores de infraestruturas. Empresas ferroviárias incluindo os operadores de instalações de serviço.
	Transporte marítimo e por vias navegáveis interiores.	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias. Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos. Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias. Operadores de sistemas de transporte inteligentes.
Bancário	—	Instituições de crédito.
Infraestruturas do mercado financeiro	—	Operadores de plataformas de negociação. Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde.	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável.	—	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
Infraestruturas digitais	—	Pontos de troca de tráfego. Prestadores de serviços de Sistema de Nomes de Domínio (DNS). Registos de nomes de domínio de topo.

Figura 2.1: Operadores de serviços essenciais

Quanto a requisitos de segurança é referido que a Administração Pública, os operadores de infraestruturas críticas e operadores de serviços essenciais devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam. Por seu lado, os prestadores de serviços digitais identificam e tomam as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços digitais.

É mencionado que os requisitos de segurança são definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

Devem ser tomadas as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados, reduzindo ao mínimo o seu impacto e assegurando a continuidade dos serviços.

As medidas devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes e os seguintes fatores:

- A segurança dos sistemas e das instalações;
- O tratamento dos incidentes;
- A gestão da continuidade das atividades;
- O acompanhamento, a auditoria e os testes realizados;
- A conformidade com as normas internacionais.

A presente legislação vem colocar novas exigências às organizações que pelas atividades e serviços que prestam passam a estar enquadradas num dos grupos referidos no âmbito da aplicação e que até então não necessitavam de reportar incidentes à autoridade nacional de cibersegurança, o CNCS. Com esta alteração legislativa, a comunicação de incidentes de cibersegurança passa a ser obrigatória, desde que cumpra um conjunto de parâmetros, e caso não o façam podem incorrer em penalizações.

2.2.4 Estratégia Nacional de Segurança do Ciberespaço

Portugal dispõe de uma Estratégia Nacional da Segurança do Ciberespaço (ENCS) que foi aprovada pela Resolução do Conselho de Ministros (RCM) n.º 36/2015 [26], de 12 de junho, e atualmente em vigor. Com o compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

A ENCS define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional e é aprovada por resolução do Conselho de Ministros, sob proposta do Primeiro - Ministro, ouvido o Conselho Superior de Segurança do Ciberespaço [15]. A sua orientação geral e específica é traduzida em seis eixos de intervenção.

No âmbito deste trabalho, focamo-nos no seu Eixo 3 - Proteção do ciberespaço e das infraestruturas, que prevê: as ameaças às infraestruturas e aos sistemas de informação são dirigidas simultaneamente às entidades públicas e privadas e aos cidadãos. Os serviços públicos servem de exemplo para a sociedade e devem ser capazes de melhorar a proteção dos sistemas de informação e da informação pelos quais são responsáveis. No âmbito da proteção do ciberespaço e de infraestruturas devem ser adotadas as seguintes medidas:

- Avaliar a maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação, no que respeita à segurança do ciberespaço;
- Promover a adaptação e melhoria contínua da segurança dos sistemas de informação das entidades públicas, dos operadores das infraestruturas críticas e dos serviços vitais de informação, para assegurar uma maior resiliência (capacidade de sobrevivência) nacional, adaptando-os aos novos riscos e ameaças do ciberespaço;
- Analisar o ambiente de informação, para tentar antecipar eventuais ataques e tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos e analisando e antecipando ameaças;

- Desenvolver a capacidade de deteção de ataques aos sistemas de informação, especialmente os das entidades públicas e as infraestruturas críticas nacionais, a qual deve permitir alertar as entidades competentes, ajudar a entender a natureza dos ataques e criar as necessárias contra-medidas;
- Promover a aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas;
- Incluir medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais, seguindo uma abordagem baseada na gestão de risco;
- Incluir medidas para fazer face a ameaças no ciberespaço nos planos de segurança dos operadores de infraestruturas críticas nacionais e europeias;
- Promover a utilização de normas de segurança da informação nas infraestruturas e sistemas de informação e de comunicação das entidades públicas. A adoção de normas e boas práticas de segurança do ciberespaço funcionam, simultaneamente, como mecanismo de harmonização e de interoperabilidade e como instrumento de medida por referência;
- Promover uma política de segurança da informação para as entidades públicas e criar instâncias que garantam a segurança da informação em todas essas entidades que acedam a informação sensível, a dados pessoais ou prestem serviços em linha considerados críticos, devendo a identificação das medidas de aplicação da política de segurança seguir uma abordagem de gestão de risco, de acordo com as melhores práticas internacionais;
- Reforçar as capacidades de prevenção, deteção e reação a incidentes de segurança do ciberespaço. Os operadores de infraestruturas críticas têm o dever de reportar falhas e interferências de segurança do ciberespaço nos seus sistemas. Por outro lado, deve ser estabelecido, em cada um destes operadores, um conjunto de meios técnicos e humanos mínimos dedicados à função de segurança do ciberespaço. Estes meios devem funcionar em rede dentro e fora do setor de atividade;
- Avaliar e desenvolver os quadros regulamentares setoriais;
- Adaptar a legislação nacional, de forma a incorporar a evolução tecnológica e as novas práticas;
- Garantir a proteção das infraestruturas de informação críticas, através de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN).

É referido que o CNCS, enquanto coordenador operacional, deve desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas públicas e das infraestruturas críticas, com vista à prevenção de e à reação a incidentes de cibersegurança.

2.3 Normas e guias

Na literatura encontramos referências a diversos normas e guias que descrevem as melhores práticas para a gestão de incidentes. Segundo *C. Hove et al.* [27] entre os mais conhecidos encontram-se a norma ISO/IEC 27035 [28][29], *Computer Security Incident Handling Guide* do NIST [8], *ITIL Incident Management* do ITIL [30], *Good Practice Guide for Incident Management* da ENISA [2] e *The Incident Handlers Handbook* da SANS [31]. Para além dos mencionados foram refenciados, durante as entrevistas, mais alguns documentos com interesse que passaremos a analisar.

2.3.1 Modelo de maturidade de reação

O CNCS, com o objetivo de dotar as entidades do Estado e os operadores de infraestruturas críticas nacionais com as valências mínimas para a análise, a mitigação e a resolução de incidentes de segurança no ciberespaço, definiu um conjunto de capacidades técnicas, humanas e processuais.

O CNCS tem como objetivo estratégico assegurar a existência de capacidades técnicas e humanas, bem como os processos necessários para uma eficaz deteção, bloqueio e resposta a incidentes de cibersegurança, nas entidades do Estado e operadores de infraestruturas críticas. Para concretizar esse objetivo foi estabelecido um plano para o desenvolvimento faseado de um conjunto de capacidades mínimas em todas as entidades do Estado e, com isso, melhorar a sua capacidade de deteção e resposta a incidentes.

O modelo de maturidade de reação [32] permite avaliar as várias entidades quanto ao seu grau de maturidade em matéria de resposta a incidentes. Apresenta um plano, composto por cinco fases, para o desenvolvimento das várias capacidades. O processo de desenvolvimento de capacidades mínimas para a reação a incidentes de cibersegurança permite uma avaliação contínua de cada uma das entidades relativamente ao seu grau de maturidade numa escala de 1 (um) a 5 (cinco).

A primeira fase é preparatória e o objetivo é estabelecer a cooperação entre a entidade e o CNCS. Na fase seguinte serão desenvolvidos os meios técnicos de deteção e análise de incidentes. Numa terceira fase, a formação dos recursos humanos da entidade para que tirem partido desses mesmos meios. A penúltima fase consiste em criar procedimentos e políticas que definam e otimizem as capacidades da equipa que estará encarregue da resposta a incidentes. Finalmente, a última fase é opcional e consiste em criar uma equipa dedicada à reação a incidentes que participe em exercícios que ponham à prova os seus procedimentos e capacidades e contribua para a comunidade nacional de cibersegurança.

Finda a execução desse plano é esperado que cada uma das entidades possua as seguintes capacidades/funcionalidades desenvolvidas:

- Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança;
- Tenha identificadas as áreas de atividade e serviços considerados críticos e realize gestão de ativos para as mesmas;
- Colete e armazene metadados de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes;
- Possua um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos ciberataques mais comuns;
- Possua os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses necessárias e articule com eficácia com o CNCS;
- Tenha aprovados e implementados procedimentos internos de resposta a incidentes de cibersegurança;
- Tenha definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de cibersegurança.

As entidades de maior dimensão ou que executam funções críticas deverão ter a sua função de resposta a incidentes assegurada por uma equipa dedicada, vulgarmente designada de CSIRT. Estas entidades deverão possuir ainda as seguintes capacidades:

- Uma equipa dedicada à reação a incidentes de cibersegurança;
- Colaboração em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT;
- Participação em exercícios nacionais e internacionais de cibersegurança.

2.3.2 Taxonomia

Como referido na RNCSIRT [16], na resposta a incidentes de segurança informática, onde a coordenação entre vários intervenientes é essencial para o seu sucesso, a utilização de uma taxonomia comum [16] para a classificação de incidentes. A classificação de incidentes deverá ser feita de acordo com o "Tipo de Incidente" e "Tipo de Evento".

A Taxonomia Comum da Rede Nacional de CSIRT é também usada na rede europeia de CSIRT [33]. Consiste numa clarificação de conceitos e base comum em que quem a usa fala a mesma linguagem. Traduz-se em interoperabilidade entre diferentes atores [34].

2.3.3 Traffic Light Protocol - TLP

A partilha e troca de informações deve seguir algumas regras dado que nem toda a informação tem o mesmo nível de sensibilidade e deve ter uma classificação diferenciada. O Traffic Light Protocol (TLP) é o protocolo de partilha adotado pelo FIRST [35] e recomendado pela Agência Europeia para a Segurança das Redes e da Informação (ENISA) [36]. Este protocolo associa a cada incidente uma de quatro cores, classificando-o quanto aos limites de partilha da informação. As cores usadas são TLP:RED, TLP:AMBER, TLP:GREEN e TLP:WHITE e a seguir descrevemos o seu significado e aplicação:

- TLP:RED = não é para divulgação, restrito apenas aos participantes. As fontes podem usar o TLP:RED quando as informações não puderem ser efetivamente tratadas por outras partes, e podem levar a impactos na privacidade, reputação ou operações de uma parte, se usadas incorretamente. Os destinatários não podem compartilhar as informações do TLP:RED com quaisquer pessoas fora da troca específica, reunião ou conversa em que foram originalmente divulgadas. No contexto de uma reunião, por exemplo, a informação TLP:RED é limitada aos presentes na reunião. Na maioria das circunstâncias, o TLP:RED deve ser trocado verbalmente ou pessoalmente.
- TLP:AMBER = divulgação limitada, restrita às organizações dos participantes. As fontes podem usar o TLP:AMBER quando as informações exigem que o suporte seja efetivamente tratado, mas ainda traz riscos à privacidade, reputação ou operações se compartilhadas fora das organizações envolvidas. Os destinatários só podem compartilhar informações de TLP:AMBER com membros de sua própria organização e com as partes que precisam conhecer as informações para se proteger ou evitar mais danos. As fontes têm liberdade para especificar outros limites pretendidos de partilha e esses devem ser respeitados.

- TLP:GREEN = divulgação limitada, restrita à comunidade. As fontes podem usar TLP:GREEN quando a informação é útil para a consciencialização de todas as organizações participantes, bem como com os pares dentro da comunidade ou setor mais amplo. Os destinatários podem compartilhar as informações de TLP:GREEN com colegas e organizações parceiras no seu setor ou comunidade, mas não através de canais publicamente acessíveis. As informações nesta categoria podem circular dentro de uma comunidade particular. TLP:GREEN a informação não pode ser divulgada para fora da comunidade.
- TLP: WHITE = a divulgação não é limitada. As fontes podem usar o TLP:WHITE quando as informações têm risco mínimo ou nenhum risco previsível de uso indevido, de acordo com as regras e procedimentos aplicáveis para divulgação pública. Sujeito às regras padrão de direitos de autor, as informações do TLP:WHITE podem ser distribuídas sem restrições.

2.3.4 SIM3

O *Security Incident Management Maturity Model (SIM3)* [37], consiste num modelo de referência para fazer avaliação e certificação da maturidade da CSIRT de acordo com os parâmetros do SIM3. O modelo identifica 40 parâmetros a serem verificados e avaliados em quatro categorias de parâmetros, que se traduzem em Organização, Pessoas, Ferramentas e Processos. Para cada um deles é especificado um nível de 0 a 4.

A ENISA [38] disponibiliza uma ferramenta online com uma visão abrangente sobre os parâmetros de avaliação, para que cada CSIRT faça a avaliação/autoavaliação da maturidade de onde pode ser obtido o resultado da mesma nos termos do SIM3. A avaliação consiste no preenchimento de um questionário, em que as respostas estão pré-estabelecidas e devem ser selecionadas as que se adaptam à realidade da organização, de acordo com o que for mais adequado para todos os parâmetros do modelo. Quando estiver completo é feito um mapeamento para a escala proposta de maturidade, com as etapas básica, intermediária e certificável.

2.3.5 ITIL

A *IT Infrastructure Library (ITIL)* é uma *framework* de gestão de serviços de TI com um conjunto de práticas que procura alinhar os serviços com as necessidades do negócio. Os processos ITIL são agrupados em etapas: *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* e *Continual Service Improvement*. Cada uma das etapas é focada numa fase específica do ciclo de vida de um serviço.

A Gestão de Incidentes é apenas um processo na estrutura de *Service Operation*. Neste processo, o propósito é restaurar o normal funcionamento o mais rápido quanto possível e minimizar os impactos negativos nas operações do negócio, assegurando que os níveis e qualidade do serviço são mantidos. O objetivo principal é que os incidentes reportados pelo utilizador transitem de um estado de reportado para o estado de fechado[30] .

A ITIL não define formalmente um incidente de segurança[39]. Define um incidente como uma interrupção não planeada de um serviço de TI ou redução da qualidade de um serviço de TI. A falha de um *Configuration Item* que ainda não afetou o serviço também é um incidente [40].

Segundo R. Pereira e M. M. da Silva [41], a ITIL é a *framework* de boas práticas mais popular para gerir serviços de TI. No entanto, a sua implementação não é apenas muito difícil, mas também não há recomendações e diretrizes para isso. Como resultado, as implementações de ITIL são geralmente longas, caras e arriscadas.

2.3.6 COBIT

O COBIT [42] é uma *framework* para desenvolver, implementar, monitorizar e melhorar práticas de governança e gestão de TI. A *framework* COBIT é publicada pelo *IT Governance Institute* e pela *Associação de Auditoria e Controle de Sistemas de Informação (ISACA)*. O objetivo da *framework* é fornecer uma linguagem comum para que os executivos de empresas comuniquem sobre metas, objetivos e resultados. A versão original, publicada em 1996, concentrou-se principalmente na auditoria. A última versão, publicada em 2013, enfatiza o valor que a governança da informação pode proporcionar ao sucesso de uma empresa.

Na versão COBIT 4.1 [43] e no objetivo do controlo DS5.6 – Definição de incidente de segurança, pretende-se que se defina e comunique claramente as características de possíveis incidentes de segurança para que possam ser devidamente classificados e tratados pelo processo de gestão de incidentes [43]. Ainda segundo a ISACA [44], este destina-se a permitir a colaboração e a partilha de informações para facilitar a compreensão e abordagem para implementar este objetivo de controlo com base no risco, valor e orientação fornecidos pelas suas práticas de controlo correspondentes.

Refira-se no COBIT5: *Enabling Processes* [45] e no processo DSS02 - *Manage Service Requests and Incidents*, com o propósito de aumentar a produtividade e minimizar as interrupções através da rápida resolução de pedidos dos utilizadores e incidentes, na documentação relacionada, a indicação à norma ISO 27002 [46] e referência à cláusula *Information security incident management*.

2.3.7 SANS

O *SANS Institute (SANS)*[3] foi estabelecido em 1989 como organização de pesquisa e educação. É internacionalmente reconhecido no âmbito da formação especializada na área da segurança da informação.

Dentro dos recursos que o SANS disponibiliza, referimos o manual *The Incident Handlers Handbook* [31], focado e limitado ao processo do tratamento de incidentes, composto por seis fases e fornece informação do que deve ser feito em cada uma delas. Em resumo, o processo compreende as fases:

- Preparação - Trata da preparação e aprontamento da equipa para responder a incidentes.
- Identificação - Trata da deteção e determina o que, dentro do que são as operações normais da organização, é um incidente.
- Contenção - Limitar o dano e prevenir outros de acontecerem.
- Erradicação - Lida com a remoção e restauração real dos sistemas afetados.
- Recuperação - Consiste em recuperar os sistemas que foram afetados, garantindo que não se provoque outro incidente.

[3]Consultar: https://www.sans.org/about/; Acedido em 20/08/2018

- Lições aprendidas - Relatar e documentar o que se passou durante o incidente e outra documentação adicional que possa ser útil em futuros incidentes e aprender com os incidentes ocorridos.

Para garantir que o processo foi cumprido deve ser realizado o preenchimento de uma lista de verificação com os itens a validar.

2.3.8 ENISA

Em 10 de março de 2004, foi criada a ENISA[4], com o objetivo de assegurar um nível elevado e eficaz de segurança da rede e da informação na comunidade e desenvolver uma cultura de rede e segurança da informação em benefício dos cidadãos, consumidores, empresas e organizações do sector público na UE, contribuindo para o bom funcionamento do mercado interno.

Em 2010, a ENISA disponibilizou o guia ENISA *Good Practice Guide for Incident Management* [2], que descreve um conjunto de boas práticas e orientações a seguir para a gestão de incidentes com ênfase no tratamento de incidentes. O foco principal deste guia é o processo de tratamento de incidentes, que envolve a deteção e registo, triagem (classificação, priorização e atribuição de incidentes), resolução, fecho e análise posterior de incidentes. O âmbito principal da gestão de incidentes são as TI e os que estão limitados a computadores, dispositivos de rede, redes e informações dentro destes equipamentos ou em trânsito.

São ainda abordados: a estrutura formal para a criação de um CERT, com a definição de funções; fluxos de trabalho; políticas de base; cooperação com outras entidades; o serviço de *outsourcing* e o reporte à gestão. Este guia fornece informações sobre como estruturar a gestão de incidentes e em especial o serviço de tratamento de incidentes, permitindo melhorar serviços ou alvo de melhoria.

Refira-se que este guia não representa necessariamente o estado da arte e pode ser atualizado de tempos a tempos e destina-se apenas a fins educativos e informativos. Tem como público alvo equipas técnicas que operam um CERT, façam tratamento de incidentes e de gestão.

As redes de comunicação e os sistemas de informação tornaram-se um fator essencial no desenvolvimento económico e social. A computação e as redes são consideradas da mesma forma que a eletricidade e o abastecimento de água. Assim, a segurança das redes de comunicação e dos sistemas de informação e a sua disponibilidade, são cada vez mais relevante para a sociedade. Isso decorre dos riscos e da complexidade dos sistemas, acidentes, erros e ataques às infraestruturas físicas que prestam esses serviços.

Estes serviços são fundamentais para o bem-estar dos cidadãos da UE e para o funcionamento das instituições governamentais, empresas e outras organizações em toda a UE.
Considera a gestão de incidentes como uma importante ferramenta de gestão global e uma necessidade. Este facto é reconhecido e suportado nas normas da série ISO 27000 [47], especificamente na ISO 27002 [46], e em *frameworks* como o ITIL e o COBIT [2].

Este guia da ENISA ajuda a fornecer uma imagem clara do processo de gestão de incidentes, de modo a que o seu conteúdo possa ser adaptado às necessidades específicas de cada organização. No entanto, o essencial permanece: prevenir, detetar e resolver incidentes e aprender continuamente com

[4]Consultar: https://www.enisa.europa.eu/about-enisa; Consultado em 10-08-2018

o processo, tendo como finalidade a melhoria contínua.

A Gestão de Incidentes compreende um conjunto de serviços mais alargados de segurança, como a capacidade de tratamento de incidentes, tratamento de vulnerabilidades, anúncios e alertas de segurança, entre outros serviços de gestão de incidentes, como se pode observar na Figura 2.2.

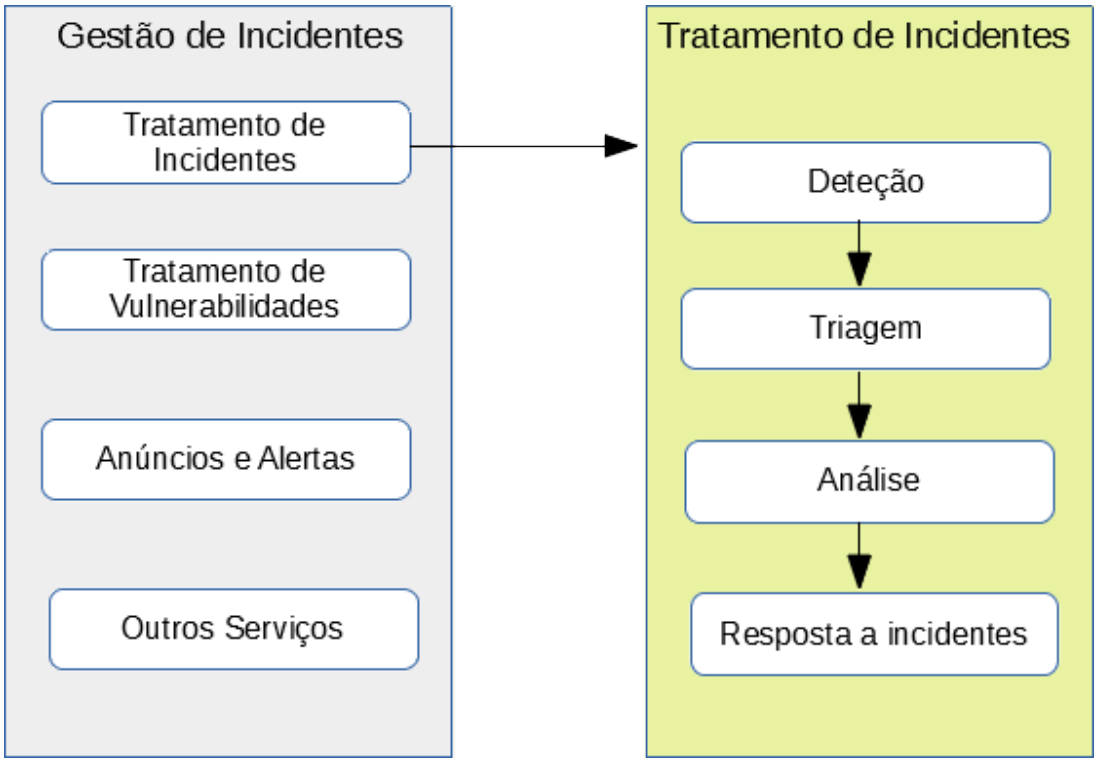

Figura 2.2: Gestão de Incidentes e Tratamento de Incidentes - Adaptado [2]

O tratamento de incidentes tem quatro componentes principais, que são apresentados na ordem em que ocorrem os incidentes. Inicialmente, um incidente é relatado ou detetado (deteção). Seguidamente, é avaliado, categorizado, priorizado e tomada uma ação (triagem). Posteriormente, é realizada uma análise sobre o incidente, para perceber o que aconteceu, quem foi afetado e analisar todas as possibilidades (análise). Finalmente, são tomadas as ações necessárias para resolver o incidente (resposta ao incidente).

2.3.9 NIST

O *National Institute of Standards and Technology (NIST)* [8] 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.

Através da *Special Publication* 800-61 *Revision* 2 [8], em 2012, publicou o *Computer Security Incident Handling Guide*, um guia com recomendações para a gestão de incidentes[5], com o objetivo de

[5]O NIST refere *computer security incident* para definir este tipo de incidente, no contexto deste trabalho e para simplificação, vamos usar o termo incidente para o referenciar

apoiar as organizações e agências federais na mitigação do risco associado aos incidentes, disponibilizando orientações sobre como responder a estes incidentes de modo eficiente e efetivo.

Medidas preventivas baseadas nos resultados da análise de risco podem reduzir o número de incidentes, mas nem todos podem ser evitados. Considera que é necessária uma capacidade de resposta a incidentes para detetar os incidentes, minimizar a perda e a destruição, corrigir as fragilidades que foram exploradas e restaurar os serviços.

Para tal, esta publicação fornece diretrizes para o tratamento de incidentes, de modo a analisar dados relacionados com incidentes e determinar a resposta apropriada para cada um. Como estabelecer uma resposta a incidentes eficaz é uma tarefa complexa, o estabelecimento de uma capacidade de resposta a incidentes requer planeamento e recursos significativos.

Estabelecer procedimentos claros para priorizar o tratamento de incidentes é fundamental, assim como implementar métodos eficazes de recolha, análise e reporte de dados.

Esta publicação auxilia as organizações no estabelecimento de recursos de resposta a incidentes de segurança de computadores e no tratamento de incidentes de maneira eficiente e eficaz.

A implementação dos seguintes requisitos e recomendações deve facilitar a resposta eficiente e eficaz aos departamentos e agências federais. As organizações devem:

- criar, aprovisionar e operar uma capacidade de resposta a incidentes formal. A lei federal exige que as agências federais notifiquem os incidentes ao US-CERT.
  O estabelecimento de uma capacidade de resposta a incidentes deve incluir as seguintes ações:
  - Criar uma política e um plano de resposta a incidentes;
  - Desenvolver procedimentos para realizar o tratamento de incidentes e seu relato;
  - Definir diretrizes para a comunicação com outras entidades sobre incidentes;
  - Escolher a estrutura da equipa de resposta a incidentes e modelo de funcionamento;
  - Estabelecer relações e linhas de comunicação entre a equipa de resposta a incidentes e outros grupos internos e externos;
  - Determinar quais os serviços que a equipa de resposta a incidentes vai fornecer;
  - Equipar e treinar a equipa de resposta a incidentes.
- reduzir a frequência de incidentes, protegendo efetivamente redes, sistemas e aplicações;
- documentar as suas diretrizes para interagir com outras em relação a incidentes;
- estar geralmente preparadas para lidar com qualquer incidente, mas devem concentrar-se em estar preparadas para lidar com incidentes que usam vetores de ataque comuns;
- enfatizar a importância da deteção e análise de incidentes em toda a organização;
- criar diretrizes escritas para a priorização de incidentes;
- usar o processo de lições aprendidas para criar valor a partir dos incidentes.

Esta diretriz foi preparada para uso das agências federais. Pode ser usada por organizações não governamentais de forma voluntária e não está sujeita a direitos de autor.

O foco principal deste documento é detetar, analisar, priorizar e tratar incidentes. As organizações são incentivadas a adaptar as diretivas e soluções recomendadas de acordo com os seus requisitos específicos de segurança e missão.

Foi criado para equipas de resposta a incidentes (CSIRTs), administradores de sistemas e de rede, equipa de segurança, equipa de suporte técnico e outros responsáveis por preparar ou responder a incidentes de segurança.

A organização deve decidir quais os serviços que a equipa de resposta a incidentes deve fornecer, quais as estruturas e os modelos de equipa que podem fornecer esses serviços. O plano de resposta ao incidente, a política e a criação de procedimentos são uma parte importante do estabelecimento de uma equipa, de modo que a resposta ao incidente seja realizada de forma eficaz, eficiente e consistente e para que a equipa tenha poderes para fazer o que precisa ser feito.

No âmbito deste guia é definido:

- **evento** é qualquer ocorrência observável num sistema ou rede;
- **incidente** de segurança é uma violação ou ameaça iminente de violação de políticas de segurança ou de práticas de segurança estabelecidas.

Os benefícios de ter uma capacidade de resposta a incidentes são:

- compatibilidade com a resposta sistemática aos incidentes para que as ações adequadas sejam tomadas. A resposta ao incidente ajuda a minimizar a perda ou o roubo de informações e a interrupção dos serviços causados por incidentes;
- capacidade de usar a informação obtida durante o tratamento de incidentes para uma melhor preparação para lidar com incidentes futuros e fornecer proteção mais eficaz para sistemas e dados;
- ajudar a lidar adequadamente com problemas legais que podem surgir durante os incidentes.

A política que rege a resposta a incidentes é específica para a organização.

Este guia detalha o processo de tratamento de incidentes em 4 fases:

- **Preparação**, estabelecer uma capacidade de resposta a incidentes, de modo a que a organização esteja pronta para responder a incidentes, evitando incidentes, garantindo que sistemas, redes e aplicativos sejam seguros.
- **Deteção e Análise**, os incidentes podem ser detetados por diversos meios, vindos de alertas, *logs* ou detetados e relatados pelos utilizadores. As organizações devem estar geralmente preparadas para lidar com qualquer incidente. A equipa de resposta a incidentes deve analisar e validar cada incidente, seguindo um processo pré-definido e documentando cada etapa realizada. A análise inicial deve fornecer informações suficientes para que a equipa priorize as atividades seguintes, como a contenção do incidente e uma análise mais profunda aos seus efeitos.

- **Contenção, Irradicação e Recuperação**, a contenção deve ser feita para limitar os efeitos do incidente. Essas decisões são fáceis de fazer se houver estratégias e procedimentos estabelecidos para conter o incidente. As estratégias de contenção variam de acordo com o tipo de incidente. Depois da contenção, a erradicação pode ser necessária para eliminar componentes do incidente, bem como identificar as vulnerabilidades que foram exploradas.

  Durante a erradicação, é importante identificar o que foi afetado dentro da organização para ser remediado. Em alguns incidentes, a erradicação pode ou é executada durante a recuperação. Na recuperação, os administradores restauram os sistemas para operação normal, confirmam que estão a funcionar normalmente e corrigem vulnerabilidades para evitar incidentes semelhantes e futuros.

- **Atividade Pós-Incidente**, uma das partes mais importantes da resposta a incidentes é frequentemente omitida. Analisar o que ocorreu, o que foi feito, como é que funcionou a equipa. Aprender e melhorar, medidas de segurança que podem ser adaptadas e melhorias ao próprio processo de tratamento de incidentes.

2.3.10 ISO/IEC 27035

A norma ISO/IEC 27035 [28] intitulada "Tecnologias de informação – Técnicas de segurança – Gestão de incidentes de segurança da informação" faz parte e complementa a série ISO/IEC 27000 [47], sistemas de gestão de segurança da informação, e a sua última versão foi publicada em 2016.

Apresenta conceitos básicos e as fases de gestão de incidentes e combina esses conceitos com os princípios de uma abordagem estruturada para detetar, reportar e relatar, avaliar e responder a incidentes, aplicando as lições aprendidas.

As políticas de segurança da informação ou controlos por si só não garantem a proteção total da informação, sistemas de informação, serviços ou redes. Depois dos controlos serem implementados, as vulnerabilidades residuais provavelmente ainda irão permanecer e podem reduzir a eficácia da segurança da informação e facilitar a ocorrência futura de incidentes de cibersegurança.

A insuficiente preparação de uma organização para lidar com tais incidentes fará com que qualquer resposta seja menos efetiva e aumente o grau do potencial impacto.

Portanto, é essencial que qualquer organização que pretenda um programa de segurança da informação tenha uma abordagem estruturada e planeada para:

- detetar, relatar e avaliar incidentes;
- responder a incidentes, incluindo a ativação de controlos apropriados para prevenir, reduzir e recuperar impactos;
- reportar vulnerabilidades de segurança da informação, para que possam ser avaliadas e tratadas adequadamente;
- aprender com incidentes e vulnerabilidades de segurança da informação, instituir controlos preventivos e aperfeiçoar a abordagem geral da gestão de incidentes de cibersegurança.

Com o objetivo de alcançar essa abordagem planeada, a ISO/IEC 27035 fornece orientação sobre os aspetos da gestão de incidentes nas suas partes correspondentes.

- Parte 1: ISO/IEC 27035-1 [28], Princípios de gestão de incidentes, apresenta conceitos básicos e fases da gestão de incidentes de segurança da informação e como melhorar a gestão de incidentes. Esta parte combina esses conceitos com princípios numa abordagem estruturada para detetar, reportar, avaliar e responder a incidentes e aplicar as lições aprendidas.

- Parte 2: ISO/IEC 27035-2 [29], Diretrizes para planear e preparar para a resposta a incidentes, descreve como planear e preparar para a resposta a incidentes. Esta parte abrange as fases ”Planear e Preparar” e ”Lições Aprendidas” do modelo apresentado na ISO/IEC 27035-1.

A norma ISO/IEC 27035 destina-se a complementar outros *standards* e documentos que fornecem orientação sobre a investigação e a preparação para investigar incidentes. É uma referência para certos princípios fundamentais que visam assegurar que as ferramentas, técnicas e métodos possam ser selecionados de forma adequada e mostrados adequados para o propósito.

Os princípios apresentados na norma ISO/IEC 27035 são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. As organizações podem ajustar as orientações de acordo com o seu tipo, tamanho e natureza do negócio em relação à situação de risco.

No âmbito da norma ISO/IEC 27035-1:2016 é definido:

- **evento** de segurança da informação como uma ocorrência indicando uma possível violação da segurança da informação ou falha nos controlos,

- **incidente** de segurança da informação como um ou vários eventos de segurança de informação relacionados e identificados que podem prejudicar os ativos de uma organização ou comprometer as suas operações,

- **gestão de incidentes** de segurança da informação, como o exercício de uma abordagem consistente e eficaz para o tratamento de incidentes de segurança da informação.

Os incidentes podem ser deliberados ou acidentais e podem ser ou não causados por meios técnicos.

Como parte da estratégia geral de segurança da informação de uma organização, devem ser colocados controlos e procedimentos para permitir uma abordagem estruturada e planeada para a gestão de incidentes. O objetivo principal é evitar e/ou conter o impacto de incidentes, a fim de minimizar o dano direto e indireto no seu funcionamento.

Os objetivos específicos de uma abordagem estruturada e planeada para a gestão de incidentes devem incluir o seguinte:

- os eventos de segurança da informação são detetados e tratados de forma eficiente, em particular, decidindo quando devem ser classificados como incidentes de segurança da informação;

- os incidentes identificados são avaliados e respondidos de modo apropriado e eficiente;

- os efeitos adversos dos incidentes de segurança da informação na organização e suas operações são minimizados por controlos apropriados como parte da resposta ao incidente;

- é estabelecido um vínculo com elementos relevantes da gestão de crises e gestão da continuidade de negócio através de um processo de escalamento;

- vulnerabilidades de segurança da informação são avaliadas e tratadas adequadamente para prevenir ou reduzir incidentes;
- as lições aprendidas de incidentes, vulnerabilidades e sua gestão. Este mecanismo de feedback destina-se a aumentar as possibilidades de prevenir futuros incidentes, melhorar a implementação e o uso dos controlos de segurança da informação e melhorar o plano geral de gestão de incidentes de segurança.

Outro objetivo associado a esta parte da norma, ISO/IEC 27035-1:2016, é que disponibiliza as orientações necessárias às organizações que pretendam preencher os requisitos definidos na ISO/IEC 27001 [48] e como um complemento à gestão de incidentes abordada na norma ISO/IEC 27002 [46].

Uma abordagem estruturada para a gestão de incidentes pode gerar benefícios significativos, tais como:

- Melhorar a segurança geral da informação;
- Reduzir os impactos negativos na atividade;
- Fortalecer o foco na prevenção de incidentes;
- Melhorar a priorização;
- Suporte à recolha de provas e investigação;
- Contribuir para justificar orçamentos e recursos;
- Melhorar os resultados da gestão e da avaliação do risco;
- Fornecer informações sobre a segurança da informação e material do programa de treino;
- Fornecer informações para a política de segurança da informação e revisões da documentação relacionada.

Para se atingirem os objetivos indicados, a gestão de incidentes, que esta norma apresenta nas suas partes, deve seguir as suas cinco fases distintas e que são: Planear e Preparar, Deteção e Reporte, Avaliação e Decisão, Respostas e Lições Aprendidas. Numa perspetiva de alto nível podemos indicar algumas das atividades que podem ser realizadas em cada fase:

- **Planear e Preparar**, a gestão de incidentes requer um adequado planeamento e preparação, realizando atividades preparatórias tais como: formular e produzir uma política de gestão de incidentes e comprometimento da gestão de topo, análise de risco, plano de gestão de incidentes, estabelecimento de equipa de resposta a incidentes, plano de testes e outros;
- **Deteção e Reporte**, envolve a deteção, recolha de informação associada a eventos e vulnerabilidades de modo manual ou automática. Monitorização dos sistemas e redes sob responsabilidade, deteção e alertas de atividades suspeitas, reportar eventos de segurança;
- **Avaliação e Decisão**, esta fase envolve a avaliação da informação associada à ocorrência de eventos e a decisão de os classificar como incidentes;
- **Respostas**, corresponde a responder de acordo com as ações determinadas na fase anterior. De acordo com essas decisões, as respostas podem ser imediatas, em tempo real e algumas também podem envolver investigação;

- **Lições Aprendidas**, ocorre quando os incidentes são resolvidos. Devem ser extraídas as lições aprendidas sobre como os incidentes e vulnerabilidades foram tratados, que melhorias podem ser introduzidas no processo e em situações futuras.

Capítulo 3

Entrevistas

Partindo da análise à literatura e ao quadro legal identificados, elaborámos um conjunto de questões que foram feitas, através de entrevistas, a especialistas na área da cibersegurança. As questões foram elaboradas tendo em conta aquilo que é indicado como sendo o recomendado existir para se fazer gestão de incidentes. O objetivo dessas entrevistas foi por um lado recolher as respostas às questões apresentadas, e daí extrair causas que levam à insuficiente preparação das organizações para esta temática, e por outro recolher outros contributos relevantes para a definição do método.

As entrevistas realizadas, no total de dez, foram respondidas presencialmente por nove dos entrevistados e somente um dos entrevistados respondeu por escrito.

3.1 Enquadramento

Os dez especialistas foram selecionados a partir de diferentes setores e organizações como veremos mais à frente. Na escolha e seleção dos entrevistados procurou-se diversificar os perfis, as entidades a que pertencem, funções exercidas e os anos de experiência. Pretendia-se que as respostas obtidas fossem diversificadas e abrangentes.

A estrutura da entrevista era composta por duas secções. Na primeira secção, fizemos o enquadramento dos entrevistados, em que questionámos dados de informação pessoal referentes ao nível de escolaridade, cargo ou função exercida, anos de experiência em segurança/cibersegurança e o sector a que pertenciam. Na segunda secção, foram apresentadas as questões sobre incidentes.

Depois de realizadas e concluídas as entrevistas fizemos o tratamento e a extração dos contributos a partir das respostas dadas para serem integrados neste trabalho.

O guião da entrevista realizada encontra-se no Anexo A.

3.2 Respostas

Do universo de entrevistados verificámos que relativamente ao nível de escolaridade a maioria possui Mestrado, seis para sermos concretos, três possuem Licenciatura e um possui Doutoramento, tal como mostra o gráfico da Figura 3.1.

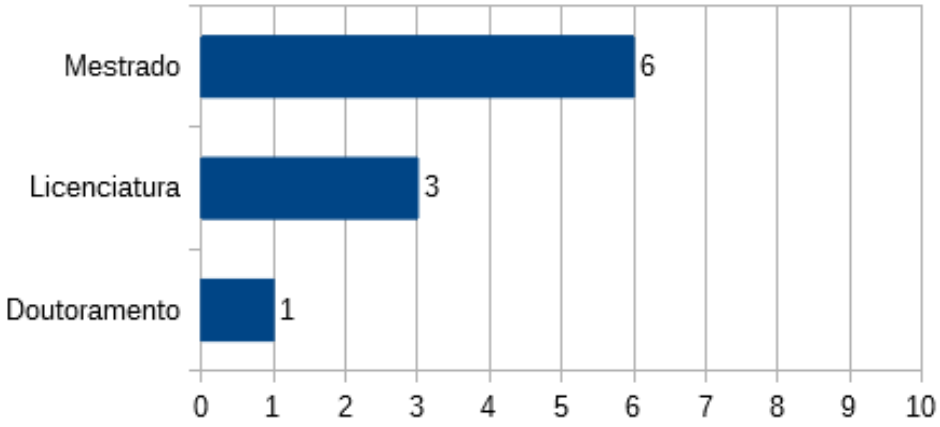

Figura 3.1: Formação académica

Relativamente ao cargo/função exercido(a) dos entrevistados, referimos que cinco desempenham cargos de Chefia Intermédia, dois a função de Consultor de Cibersegurança, um a função de Professor Universitário, um o cargo de Diretor de Serviço e um o cargo de *Chief Executive Officer (CEO)*, como pode ser observado no gráfico da Figura 3.2.

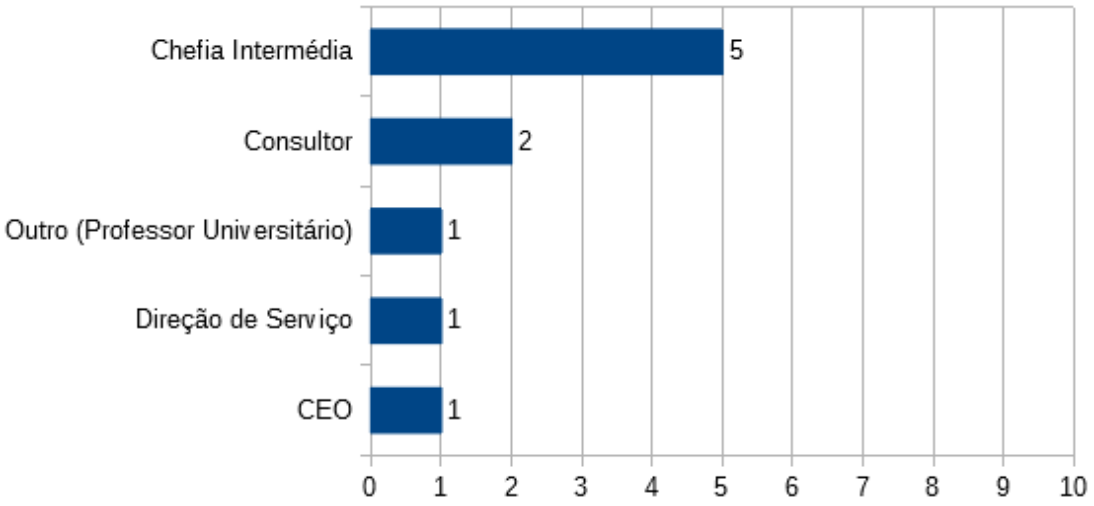

Figura 3.2: Cargo/Função exercido(a)

Quanto aos anos de experiência em segurança/cibersegurança, salvo um dos entrevistados, todos têm mais de cinco anos de experiência nesta área e relevamos dois com mais de vinte. Estes dados podem ser observados no gráfico da Figura 3.3.

Consideramos estes dados interessantes e significam que a seleção dos entrevistados foi conduzida no sentido de obter contributos relevantes baseados no conhecimento e experiência destas pessoas na área da cibersegurança.

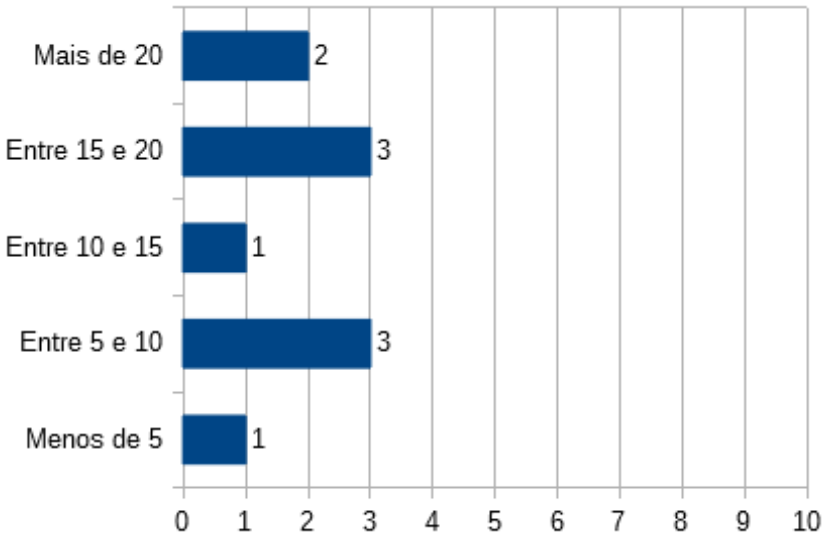

Figura 3.3: Anos de experiência

Na última questão da primeira seção da entrevista obtivemos os dados referentes ao setor a que pertenciam e exerciam a sua atividade. De acordo com o gráfico da Figura 3.4 a maioria dos entrevistados, neste caso sete, exerciam as suas funções no setor público e os restantes no setor privado.

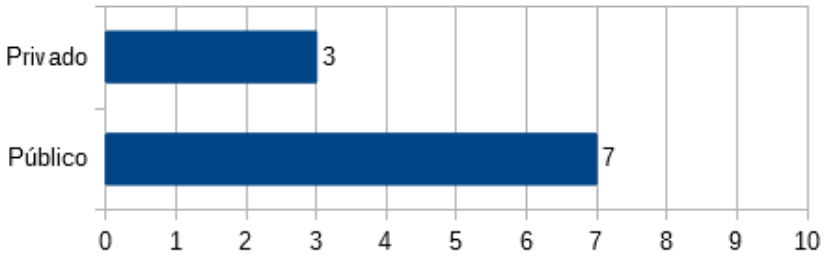

Figura 3.4: Setor de atividade

Questão 1: O que entende por incidente de cibersegurança?

A esta questão um dos entrevistados respondeu que, *"(...) entende-se (...) uma ação ou conjunto de ações desenvolvidas que resulte ou possa resultar na perda de confidencialidade, integridade, ou desempenho de uma rede de comunicação, de dados ou sistema (...)"*.

Complementando, outros entrevistados referiram o *"(...) funcionamento anómalo (...) que consegue comprometer (...) parâmetros da segurança de informação (...)*, *"(...) a disponibilidade dos dados e dos serviços (...)"*.

Mencionaram ainda *"(...) evento, em que há sempre intervenção humana(...)"*, *"(...) atingem e têm impacto em infraestruturas tecnológicas(...)"*, *"(...) conjunto de acontecimentos que (...) criam disrupção no normal funcionamento de sistemas. Sistemas compreende-se pessoas, tecnologias e processos(...)"*, *"(...) qualquer coisa que permite violar uma política de segurança (...)"*, *"(...) suspeita ou intrusão que não se tenha verificado ainda o referido impacto, mas que deve ser trabalhado ou tratado como um incidente dentro da organização."*.

Questão 2: Os incidentes de cibersegurança, no seu entender, são essencialmente causados

por questões técnicas ou por questões comportamentais? Justifique.

A maioria dos entrevistados reconheceu que os incidentes são essencialmente causados por *"(...) questões comportamentais(...)*.

Alguns dos entrevistados referiram que: *"(...) as comportamentais são a base porque mesmo as falhas técnicas têm por base um comportamento errado de quem desenvolveu a tecnologia, que a configurou e a implementou (...)"*; *"(...) questões comportamentais que tiram partido de fragilidades técnicas. Levam as pessoas a ter (...) comportamentos que a componente técnica não protege (...)"*; *"(...) são maus comportamentos (...), comportamentos inadequados ou desajustados(...) que as vulnerabilidades da tecnologia tiram partido (...)"*; *"(...) as pessoas não sabem que aquele equipamento tem um determinado problema ou tem aquela vulnerabilidade e é explorada por aí (...)"*.

Referiram ainda que: *"O elo mais fraco será o ser humano(...)"*, *"(...) todos cometemos erros e esses erros levam a falhas (...) que se forem exploradas levam a incidentes (...)"*; *"(...) não só na perspetiva dos utilizadores mas também (...) administradores de sistemas, (...) técnicos que administram as soluções, por não terem um comportamento que privilegie a segurança em todo o ciclo de vida dos sistemas (...)"*; *"(...) não adoção de meios técnicos adequados é uma dessas causas(...)"*; *"(...) comportamentais têm de ser recorrentemente validadas e treinadas (...) é preciso estar permanentemente a educar, fazer ações de sensibilização e mudar comportamentos de segurança (...)"*.

Um dos entrevistados referiu que *"(...) as organizações estão a adotar (...) tecnologias diferentes, (...) legadas que mantemos por anos, tecnologias novas, telemóveis e outros, (...) riscos inerentes à tecnologia e não ao utilizador da tecnologia. (...) há muito e mais complexo, (...) mais funcionalidades (...) integração, (...) sofisticação (...) tudo tem riscos (...)"*.

Outro dos entrevistados respondeu que *"(...) os incidentes vão ter intervenção de pessoas (...), na motivação (...) está a vontade, a capacidade e a oportunidade de agir (...), nessa vontade (...) há (...) dinheiro, ideologia, coação, ego e ressentimento (...)*. Referiu questões, que no seu entender, devem ser respondidas quando ocorre um incidente *"(...) O quê? Onde? Quando? Como? Quem? Porquê? Quanto? (...)"*.

Questão 3: Entende que deve existir uma política de cibersegurança transversal suportada e aprovada pelo órgão máximo da organização? Na sua organização existe e é aplicada? Se aplicável, quem a aprovou?

A esta questão todos os entrevistados responderam que *"(...) tem de haver uma política e ser transversal (...)" "(...) à organização e aprovada ao nível máximo (...)"*.

Um dos entrevistados referiu que *"(...) A política diz o que fazer. (...) tem de haver doutrina que nos diga como fazer. (...) é importante (...) uma doutrina nacional ou organizacional (...) para depois a política instanciar essa doutrina. (...) a política de cibersegurança não se confina a aspetos de natureza técnica (...) ser transversal a todas as políticas da organização. A nossa política decorre da ENCS, com normas técnicas, conjunto de boas práticas e newsletters (...)"*.

Complementando, outro entrevistado referiu que *"Não funciona se não for assim. (...) qualquer temática no âmbito da segurança da informação tem de ser holística ou transversal e contínua no*

tempo (...). É crucial o commitment do top management, quer seja numa organização pública ou privada. (...) empowerment na aplicação de controlos, (...) especificação de políticas, procedimentos e ação numa situação de crise (...). Sim temos uma política e foi assinada pelo Board (...).” Foi referido por outro entrevistado *”(...) deve haver uma política (...) que é aplicada a toda a organização (...) pode ser adaptada a casos específicos ou a determinadas áreas (...)”*.

Como referiu outro entrevistado *”(...) a segurança não é um problema de Information Tecnology (IT) é um problema da organização (...) o risco que induz é um risco para o negócio da organização e (...) tem de ser visto como todos os riscos de qualquer atividade seja pública, privada, comercial ou sem fins lucrativos. (...) gestão de topo o que faz é gerir riscos (...) a cibersegurança é mais um risco (...). Internamente existe uma política de cibersegurança e é aprovada pelo CEO da empresa (...) como prestadora de serviços (...) temos organizações que estão muito bem, (...) têm já um staff alocado à área da cibersegurança (...).”*

E para complementar, acrescentou*”(...) há muitas empresas que não têm e não está substanciado (...) não há evidências, nada escrito formalmente suportado nas políticas implementadas(...). Na (...) perspetiva de resposta a incidentes (...) e na implementação de medidas de controlo, deixa-nos no vazio para implementação de medidas básicas (...).”*

Um dos entrevistados respondeu que faltam *”(...) políticas transversais que suportem e orientem as organizações atendendo à sua dimensão. (...) necessidade é cada vez maior. Na (...) organização já existem algumas políticas. Não existe uma política de cibersegurança (...) estamos a trabalhar (...).”*

Um dos entrevistados referiu que na sua organização existe uma *”(...) política (...) global, (...) para toda a empresa. (...) estamos a preparar a certificação ISO 27001. (...) tendo por base a política de grupo, adaptá-la ao nosso contexto e enquadramento (...), base (...) transversal (...) deve ter os pilares essenciais. (...) indicação de quais (...) as diretrizes dos serviços essenciais do grupo. Deve existir e existe, foi aprovada pela administração do grupo, (...). Existe um pelouro de tecnologia que tem um Chief Technical Officer (CTO) que aprovou esta política. (...) depois a Direção Intermédia aprova a política tal como exige a ISO 27001.”*

Na opinião de um entrevistado, *”(...) A segurança (...) vista ao nível da gestão e faz parte do negócio(...). Quem a deve desenhar deve ser um Chief Security Officer (CSO) ou equivalente. (...) definida no sentido de competências e responsabilidades sobre assets. (...) cada departamento terá necessidade de refinar a política (...) definida a nível superior (...) toda a gente siga e não se desvie. (...) recolhidos os contributos que fazem ou não sentido (...) tendo em conta a estrutura da organização. Na organização existe uma política em dados concretos. A nível geral não sei. É possível nos serviços fazer melhor.”*

Um entrevistado entendeu que a política deve ser *”(...) transversal a todas as áreas de negócio, financeira, recursos humanos, todas as áreas tradicionais de uma organização. (...) em silos verticais a cibersegurança acaba por ser uma linha horizontal transversal a todos. (...) não pode estar dependente de um dos silos mas sim de quem está acima dos silos (...) a nível máximo. Nesta organização é tomada ao nível máximo.”*

Um dos entrevistados, e na sua opinião pessoal, referiu que *”(...) a Ciberdefesa, o Serviço de Informações da República Portuguesa (SIRP), Polícia Judiciária (PJ) e o CNCS, alicerçados (...) na*

política para a parte digital. (...) há programas laterais, (...), como a Escola Segura, etc, que são do Ministério da Administração Interna (MAI), mas que são fundamentais. (...) dizer às pessoas a segurança da informação depende de pessoas, tecnologias e processos. (...) faz falta conhecimento de cibersegurança, sensibilização às pessoas e empresas.

Defendeu que devia haver *"prevenção criminal dirigida para determinados grupos alvos, crianças, pais e professores, no mínimo. Tenho pena que (...) não exista um plano nacional de prevenção. (...) deve existir uma política de cibersegurança, deve ser transversal pelo menos a estas quatro partes que referi e porquê? (...) intervêm mais diretamente na parte da soberania do estado e no combate ao crime organizado. Por causa disso é que não referi qualquer Orgão de Polícia Criminal (OPC). (...) como a legislação está configurada, tem sido atribuído por lei à Polícia Judiciária (PJ). Se for alterado (...) não impede que não haja uma articulação com os outros OPC, que devia haver, mas não há (...)".*

Questão 4: Considera que a inventariação e gestão dos ativos e serviços críticos podem contribuir para reduzir a exposição a incidentes de cibersegurança? Realizam essa inventariação e gestão de forma contínua e está atualizada?

Nesta questão, todas as respostas foram unânimes e no sentido de que *"(...) a inventariação e a gestão dos ativos é fundamental (...)"* e *"(...) contribuem para a redução dos riscos e dos incidentes de cibersegurança"*. Alguns dos entrevistados consideram *"(...) crucial inventariar os ativos e os serviços, ativos humanos e não humanos (...)*, *"(...) todos os ativos, sejam eles críticos ou não (...)". "(...) depois categorizá-los (...) para (...) introduzir e prioritizar a resposta a incidentes (...)." "(...) não há gestão de incidentes sem saber onde o incidente se está a produzir e porque é que ele se está a produzir (...)".*

Dois dos entrevistados indicam que *"(...) é preciso ter uma base dados, (...) uma Configuration Management Database (CMDB). (...) que (...) diga que ativos temos, que releases, que IP tem, que software tem lá instalado, toda a informação que (...) permita (...) do ponto de vista da cibersegurança (...) um acompanhamento daquele ativo (...) ao longo do seu ciclo de vida."*, *"(...) é preciso manter essa base de dados (...) de configurações e recursos que nos permitam saber a qualquer altura como é que se consubstancia esses recursos mais valiosos em relação aos outros (...)."*

Referiram ainda que fazem internamente a inventariação e gestão de ativos e serviços, ou estão em processo de o fazer. Duas pessoas referiram que *"Duvido é que haja muitas organizações que o façam (...)" "(...) em outras organizações públicas acredito que não o façam (...)."*

Um dos entrevistados respondeu que *(...) não temos ainda uma inventariação contínua dos ativos (...) o reajuste orgânico das entidades (...) leva a isto. Na administração pública (...) as estruturas das organizações públicas mudam (...) muito (...). Pode ter um impacto significativo. (...) fusões de organismos ou separação de organismos (...). Maturidades distintas, níveis de inventário distintos, formação distinta, passagem melhor ou pior de informação entre entidades e equipas.*

Referiu ainda *"Não haver uma normalização. (...) separação muito grande entre o (...) inventário financeiro, contabilístico de todos os ativos para aquilo que é muitas vezes inventário para fins de gestão de TI,(...) se (...) fosse visto numa ótica muito mais integrada muito do trabalho (...) poderia contribuir para o inventário de TI e evitar replicar esforços das equipas (...)"*

Na resposta de outro entrevistado é indicado que *"(...) Uma organização que tenha uma política de*

Bring Your Own Device pode tentar implementar mecanismos de minimização dos danos mas acho que não consegue fazer essa inventariação (...).”

Um dos entrevistados esclareceu que *”(...) ativos, se forem os críticos. (...) estamos (...) preocupados em explicar às Pequenas e Médias Empresas o que são (...), aí não há dinheiro para pagar a estruturas permanentes, a engenheiros (...)*. Refere que *”(...) na parte do Estado (...)”* os recursos humanos nem sempre estão preparados, tal como *”(...) numa pequena empresa familiar (...)”* em que alguém dá um *”(...) jeito (...)”*.

Aconselha utilizar a Segnac 4, *”(...) diploma que está em português acessível, é uma base, aborda segurança física, segurança lógica e seus componentes (...)”. ”(...) ativos críticos é (...) transmitir às pessoas, associações de empresários, o que (...) de dados, ficheiros, ou de informação que se for retirada ou se for estragada pode comprometer o seu local de trabalho (...).”*

Questão 5: Quer indicar uma ou mais normas ou guias para a gestão de incidentes de cibersegurança que conheça? Caso tenha indicado alguma(s), a(s) mesma(s) é(são) aplicada(s) na organização?

As respostas a esta questão foram variadas. Alguns dos entrevistados referiram o NIST, framework da NIST, ISO 27035, *workflow* da ENISA, guia de boas práticas da SANS, ISO 27001, ISO 27002, *”(...) família ISO 27000 toda, mais as análises de risco (...)”*, diretiva *Network and Information Security (NIS)* da UE, taxonomia, SIM3.

O esclarecimento dado foi que *”Há muitos guias para a resposta a incidentes (...) a organização adotou e (...) estamos muito alinhados com o NIST.” ”(...) o ISO 27035 (...) o NIST 800-61 (...) andam muito perto e a distinção se são seis ou cinco passos do ciclo, no fundo a base está lá toda. Alguns clientes alinham mais de perto com a ISO 27001 e ISO 27002 e preferem usar a ISO 27035. Como a ISO 27035 é paga e nem todos têm a certificação ISO 27001, preferem alinhar pelo NIST, que é gratuito e está disponível e há muito material publicado (...).”*

Referiram que *”(...) estes modelos são muito complexos para a maturidade das nossas organizações e das equipas (...) a necessidade de adequar o modelo standard para a realidade da organização (...)”*. Outro referiu que foram *”(...) criando (...) conhecimento interno, depois (...) adaptando à medida que foram nascendo standards. (...) alinhados com ISO 27001, ITIL e (...) estar alinhados com standards (...).”*

Um dos entrevistados clarificou a sua resposta *”Normas para gestão de incidentes há várias, (...) são guias, são modelos de referência (...) têm de ser adequados a cada entidade. Seguimos a estrutura de um CSIRT e de publicação de um CSIRT que vem nos RFC’s, seguimos o que é tradicionalmente na forma de gerir um incidente e as funções que as equipas devem ter ou as funções ou os serviços que devem prestar de acordo com o que vem na NIST (...), não tanto a ISO. (...) Mas são todas muito semelhantes e acabam por estabelecer qual é a missão do CSIRT, (...) como (...) se deve posicionar na organização (...).”*

E acrescentou *”(...) Tentar que esteja o mais no topo possível ou mais dependente do topo e depois todo o conjunto de serviços e a forma como são prestados e estruturados. A sua constituency bem definida,(...) é definida pelo modelo da organização e o modelo de gestão que se quer (...). (...) há vários modelos de maturidade e aquilo que devem ser os serviços, como (...) devem ser organizados,*

o que devo ter segundo o modelo de maturidade. O SIM3 (...) acaba por ser uma ferramenta para me avaliar, mas ao mesmo tempo que me estou a avaliar estou a perceber o que é que não tenho, tenho de perceber os meus espaços vazios, as lacunas que tenho e onde posso melhorar".

Questão 6: Faz sentido existir uma harmonização na utilização de boas práticas e normas nacionais/internacionais na forma de gerir este tipo de incidentes? Se sim, quais as que utilizam? Se não, justifique a sua resposta?

Os entrevistados, e por unanimidade, responderam que faz sentido haver harmonização pelo menos ao nível da utilização da taxonomia da Rede Nacional de CSIRT. Referiram a utilização de boas práticas mas sem caráter obrigatório e vistas como recomendações.

Indicaram alguns aspetos comuns como *"(...) comunicações seguras, protocolos de segurança que são comummente aceites, o caso do PGP, é algo que transversalmente é aceite como forma de tornar a comunicação segura (...). Pode ser usado um diferente desde que se garanta a interoperabilidade e que o CSIRT não fique fechado ao mundo (...)." "(...) requisito para uma boa cooperação é uma comunicação eficaz (...)."* Um dos entrevistados referiu que *"(...) o facto de uma organização ter um modelo feito à medida e específico é vantajoso (...)."*

A resposta de um dos entrevistados referiu *"(...) as organizações até podem ter normativos diferentes. Devem é ter uma taxonomia comum porque uma mesma coisa não representa a mesma coisa. (...) tem de haver interoperabilidade e semântica taxonómica para que as coisas funcionem (...)."*

Questão 7: A gestão e tratamento dos incidentes de cibersegurança deve seguir uma metodologia própria e bem definida ou pode ser ad-hoc? No caso da sua organização, qual é a abordagem utilizada?

Nesta questão os entrevistados foram unânimes e responderam que a gestão e tratamento dos incidentes deve seguir uma metodologia muito bem definida.

Referiram que as organizações devem ter uma *"(...) metodologia própria. É difícil ter uma metodologia única que sirva a todas as organizações(...). "(...) o objetivo é muito bem definido, reduzir ao máximo o tempo que medeia a deteção e a reação. (...) comecemos a reagir antes do incidente (...) se manifestar. (...) é difícil mas tem de ter um propósito, (...) o tratamento desses incidentes tem de ser feito não só com uma taxonomia comum mas também com um conjunto de procedimentos para reação que seja interoperável (...)."*

A resposta dada por um entrevistado referiu que utilizam uma metodologia própria e muito bem definida. *"(...) Essa é a maneira de (...) ter uma rotatividade de pessoal, e (...) retirar o fator humano. (...) o processo seja imune a alterações das pessoas e isso é uma das principais vantagens (...). Metodologia do processo em que toda a gente sabe onde é que está. Se repetirmos o processo os processos são semelhantes. Permite ter uma base de conhecimento sobre aquilo que já foi visto, sobre os incidentes que já foram tratados e aplicar a receita com otimização de esforço, automatização e fazer reajustes se se justificar(...)".*

Outra resposta indicou que *"(...) A metodologia (...) para a gestão e tratamento de incidentes deve ser sistematizada e aí (...) o plano traz vantagens. Todos seguem o mesmo procedimento, que vai ser*

rastreável, auditável e a organização ao longo do tempo vai mantendo o histórico com aquilo que vai acontecendo, do que vai fazendo (...) e assegurado do ponto de vista tecnológico. Se (...) o plano for um documento, o pessoal vai estar preocupado em resolver o incidente. (...) suportar a atividade de gestão e resposta a incidentes numa ferramenta, neste caso o ServiceNow, uma ferramenta de ticketing (...). RTIR e OTRS são outras soluções. Aquilo obriga-nos a fazer o que está estabelecido no plano."

Para além da metodologia referiram ainda que os *"(...) serviços que se prestam têm de estar bem definidos, que tipos de incidentes trato e não trato (...), como é que trato cada um dos incidentes, até onde vai o nível de serviço que presto. Papéis e responsabilidades têm de estar definidos."* Um dos entrevistados referiu como relevante a *"(...) uniformização dos reportes e de comunicação dos eventos (...)."* Um entrevistado explicou que na sua organização *"Existe um report, depois é realizada uma triagem, é efetuada uma investigação, comunicado o resultado, fechado o incidente e analisado à posteriori."*

Questão 8: A existência de uma equipa de resposta a incidentes de cibersegurança deve ter definidas as suas competências e atribuições. O mandato deve ser dado pelo topo da organização ou pelo departamento responsável pela área de TI? Justifique a sua resposta.

A resposta foi clara e unânime, o mandato *"(...) deve ser dado pelo topo da organização (...)"*.

Referiu um dos entrevistados *"(...) As questões de cibersegurança não são questões de carácter tecnológico. São questões transversais à organização, (...) têm de ser da visibilidade do topo da organização. O mandato deve ser dado pelo topo da organização, não tenho dúvidas acerca disso. Se não o for é mau."* Outro entrevistado indica que *"(...) A equipa de resposta a incidentes deve ter um comportamento idêntico ao de um auditor externo. (...) que responda ao Conselho de Administração ou ao topo. Tem de ter independência para não gerar conflitos de interesse. (...)."*

Na opinião de outro entrevistado *"(...) A segunda é um erro. Um erro grave e infelizmente é o que acontece nas organizações (...) depois as coisas não correm bem.(...) em alguns setores deve estar completamente separada do IT. (...) do compliance ou do legal.(...) o CSIRT deve ter acesso direto ao CEO ou ao próprio Board (...). Sem esse empowerment estas coisas não funcionam. (...) pode haver organizações em que esta equipa pode estar ou ser a mesma que a de TI. (...) mas que se garanta o empower quando for necessário (...)"*.

Outro contributo referiu *"(...) muitas vezes a equipa de resposta a incidentes tem de tomar (...) decisões que podem ter impacto no negócio da empresa, na atividade produtiva da organização. (...) não se pode esperar que alguém faça o percurso todo até ao topo."* Outro entrevistado acrescenta *"(...) um mandato claro com as competências e atribuições bem definidas para a equipa de resposta a incidentes (...)."*

Um entrevistado indicou que *"(...) o ideal é o topo da organização envolver a área de IT e todas as outras na gestão de incidentes (...) pessoas de diversas áreas, não só técnicos, desde jurídicos, comunicação, recursos humanos, toda a organização (...) pessoas (...) que se reconhece o seu papel na resposta a incidentes, (...) o plano e a formalização é importante à resolução do problema."*

Questão 9: O treino e a preparação da equipa de resposta a incidentes deve ser encarada como uma mais valia para a organização ou como um custo? Se a sua organização dispõe desta

equipa, como é que é encarada? Se não tem ninguém dedicado, quais são as razões para não ter?

A maioria dos entrevistados encararam o treino e a preparação da equipa de resposta a incidentes como uma mais valia para a organização.

Afirmou um dos entrevistados *"(...) é uma mais valia que acaba por trazer competências para a organização e acaba por poupar à organização (...) custos (...) com incidentes. Custos menores que os incidentes. Pode não evitar um incidente mas pode minimizar o custo que um incidente tem no negócio de organização. (...) A formação é encarada (...) é obrigatório pelo menos para a equipa (...)".*

Vários entrevistados referiram que *"(...) a formação e treino é essencial e fundamental numa equipa de resposta a incidentes (...)"*, *"(...)treinada para estar no automático, para as pessoas não serem apanhadas desprevenidas (...)"*. Um deles respondeu que *"há (...) organizações que não têm staff e (...) recorrem a empresas externas para lhes prestar esse serviço (...). A componente de resposta a incidentes tem sempre que existir e o plano de resposta a incidentes é da organização, não é do subcontratado. Tem sempre que haver uma capacidade de resposta a incidentes interna e tem de ser treinada e é essencial."*

Diversos entrevistados referiram que a resposta também é *"(...) componente comunicação porque pode ser necessário falar com órgãos de comunicação social, (...) resposta para os investidores, para o próprio Board. (...) O plano não deve existir só para apanhar pó, deve ser exercitado para se perceber se está desatualizado (...)."*

Um dos entrevistado, no acesso à formação referiu que tenta *"(...) todo o tipo de ações formativas essencialmente de qualidade e de baixo custo. O custo é na realidade, na área pública um fator preponderante. (...) tem impacto na atribuição de verbas e correspondente formação."* Ainda relacionado com a formação outro entrevistado indicou que têm *"(...) um plano de formação com um programa específico para cada tipo de colaborador (...) além do treino são realizados exercícios todos os anos. Todos os colaboradores da organização fazem formação na área de cibersegurança (...)."*

Questão 10: Tendo sido detetado um incidente, considera que deve existir uma análise detalhada para saber o que aconteceu e criar conhecimento interno para aprender e evitar situações futuras? Isso é aplicado na sua organização? Se sim, de que forma?

Foi reconhecido pelos entrevistados que tem de haver uma análise detalhada *"sobre as causas, origens e as formas como se produziu esse incidente". "(...) lógica de feedback de ciclo fechado que vai sempre contribuindo para a melhoria contínua da organização."* Numa primeira fase interessa*"(...) debelar o incidente quando surge, mitigar os seus efeitos, depois é analisá-lo e perceber que ele se manifestou daquela maneira na organização".*

Um dos entrevistados recomendou *"(...) as organizações deviam ter uma base de dados de lições identificadas e lições aprendidas para depois verter na doutrina (...) e eventualmente na política em conformidade".* Complementando, outro entrevistado referiu que se deve *"(...) incluir a noção de aprendizagem ou as coisas não funcionam (...) como uma nova ameaça que foi recolhida (...) prevenirmos outras (...) ou porque descobrimos outro vetor de ataque, uma nova abordagem a nível técnico é crucial. (...) garantir o legado e o conhecimento de milhares de incidentes tratados pela equipa".*

Outros referiram que *"(...) isso ao fim de algum tempo leva a uma base de conhecimento que serve de suporte (...),""este processo é rápido, acaba por ser uma tipificação do que vem de trás (...), é acumular esses dados para fins estatísticos e avaliar tendências". "(...) essa análise detalhada não pode ser para todo o tipo de incidente (...) deve-se à gravidade e impacto que (...) teve na organização devido à classificação que lhe é dada". "Fase em que aprendemos com os erros cometidos e deve ter um input em tomada de posições." "(...) em certas situações através da implantação de novas ferramentas".*

No âmbito da cooperação internacional, e segundo um dos entrevistados, o conhecimento criado internamente deve ser passado ao SIRP e CNCS, e se for transnacional, dependendo dos casos, informado o EC3 ou a Europol.

Questão Livre: As questões apresentadas merecem-lhe algum comentário ou deveria ter questionado algo que não foi mencionado?

A esta questão os entrevistados indicaram/propuseram *"(...) o treino que deve ser dado às pessoas que não estão ligadas à resposta a incidentes de segurança. Ás pessoas comuns da organização, que estão em departamentos e não trabalham com estes assuntos (...)." "(...) As limitações das organizações públicas, dificuldades no acesso a formação, contratação pública, gestão de orçamentos, problemas na governação do próprio estado." "Relatório modelo do CNCS e se o reporting que temos no nosso plano nos dá as respostas todas que um CNCS nos pode pedir um dia. A uniformização nas fases que suportam o plano."*

3.3 Resumo

Concluídas as dez entrevistas extraímos das respostas alguns contributos importantes que serão integrados neste trabalho.

Foi referido que o elo mais fraco será o ser humano e que os incidentes de cibersegurança são essencialmente causados por comportamentos inadequados dos utilizadores. O caminho passa por desenvolver planos de formação e treino adaptados a todos os colaboradores.

A cibersegurança tem de ser transversal a toda a organização e não estar em silos verticais. Nesta matéria, o tempo é crucial e a tomada de decisões tem de ser célere e suportada ao nível máximo da organização. É também fundamental conhecer todos os ativos da organização, por diferentes necessidades, para se poderem tomar medidas adequadas e concretas.

Para além dos contributos obtidos houve interesse em identificar algumas causas para a insuficiente preparação das organizações. Indicamos algumas das causas referidas:

- O reajuste orgânico na estrutura das organizações públicas, fusões ou separação de organismos;
- A falta de inventariação e identificação de todos os ativos;
- A falta de recursos humanos;
- A capacitação e formação dos recursos humanos;
- As limitações das organizações públicas ao nível da contratação pública e da gestão de orçamentos;

- As dificuldades no acesso a formação;
- A ausência de políticas e procedimentos;
- Os investimentos feitos aos quais não é retirado proveito.

Todos estes contributos são relevantes para a contextualização e entendimento no âmbito desta dissertação.

Capítulo 4

Proposta

Neste capítulo apresentamos a nossa proposta para solucionar o problema identificado no capítulo 1 e os objetivos que nos propomos alcançar.

De acordo com as exigências do processo de construção de um artefacto como refere a DS, construímos um método que concretiza um processo de referência para a gestão de incidentes de cibersegurança. Segundo *Hevner et al.* [1], os métodos definem processos e fornecem orientações sobre como resolver problemas. Essas orientações podem ser descrições textuais e informais das abordagens de melhores práticas ou combinações.

Esta proposta advém da literatura e do trabalho relacionado e também dos contributos obtidos de entrevistas a especialistas na matéria, traduzida na estrutura da Figura 4.1. Clarificando os componentes apresentados, as *Frameworks* correspondem às normas e guias já referidos, com foco nos documentos da ENISA, do NIST e da ISO, e os normativos referem-se ao quadro legal referenciado. Com este suporte, extraímos uma estrutura base que denominámos *Draft*, e de onde elaborámos as questões para as entrevistas. No final, e agregando a informação recolhida desses inputs construímos a Proposta.

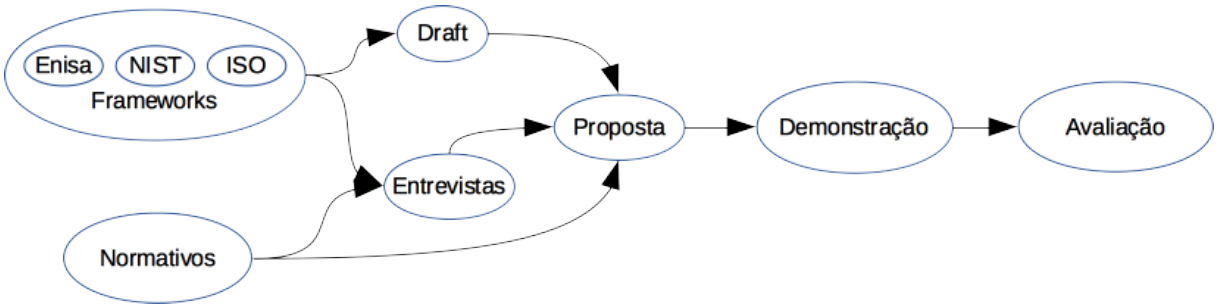

Figura 4.1: Base para a proposta

De seguida, apresentamos quais os objetivos a alcançar e o Método Proposto para os atingir.

4.1 Objetivo

O objetivo que nos propomos alcançar é o de contribuir para a implementação do processo de gestão de incidentes de cibersegurança nas organizações portuguesas. Este contributo pode significar um percurso inicial, em que ainda nada está definido e implementado, até situações mais avançadas em que já existe o processo de gestão de incidentes estabelecido e este possa introduzir melhorias.

4.2 Método Proposto

A gestão de incidentes deve ser realizada de forma metódica e ter definidas um conjunto de fases com as práticas a desenvolver.

O processo de referência proposto está alinhado com a norma ISO/IEC 27035 e segue as suas orientações. Justificamos esta decisão com base nas indicações constantes no quadro legal onde se refere *"a utilização de normas e especificações técnicas internacionalmente aceites"* [15], e *"adoção de normas e boas práticas de segurança do ciberespaço"* [26]. Também o guia da ENISA [2] refere a adoção da ISO/IEC 27002 que por sua vez remete para a norma ISO/IEC 27035.

Propomos um processo de referência constituído por cinco fases compostas por práticas e objetivos a atingir em cada uma delas. As fases que identificámos para constar no processo devem ser as seguintes: Planeamento e Preparação, Deteção e Participação, Análise e Avaliação, Resposta e Documentação, e Lições Aprendidas.

Seguidamente, detalhamos o que deve constar no processo de referência e em cada uma das suas fases.

Definição de incidente de cibersegurança - entende-se uma ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores que resulta, ou pode resultar, na perda da confidencialidade ou integridade da informação ou prejudica o desempenho de uma rede de comunicação de dados ou sistema. Normalmente um incidente de segurança das redes e da informação significa uma violação da política de segurança de uma organização [16].

4.2.1 Planeamento e Preparação

A gestão de incidentes de cibersegurança para ser eficaz e eficiente requer um planeamento e preparação adequados. Para tal, devem ser concretizadas um conjunto de práticas para que seja colocada em funcionamento. Para esta fase devem ser concretizadas as seguintes práticas:

Práticas

PP. 1 Identificar quais os objetivos, partes interessadas dentro e fora da organização, especificar o tipo de incidentes que são tratados, funções que devem ser incluídas, benefícios para a organização e para os seus departamentos, para se formular e produzir uma política de gestão de incidentes de cibersegurança transversal a toda a organização e com a aprovação, comprometimento e suporte da gestão de topo;

PP. 2 Alinhar e atualizar as políticas de segurança da informação, da gestão de risco e outras existentes ao nível da organização, dos sistemas, serviços e redes;

PP. 3 Concretizar um plano detalhado para a gestão de incidentes de cibersegurança, referindo com quem devem ser estabelecidas comunicações e como deve ser feita a divulgação de informações; Esta divulgação deve ser efetuada de acordo com o estipulado no *Traffic Light Protocol (TLP)*;

PP. 4 Constituir uma CSIRT, com treino e formação adequados e atualizados a todos os seus elementos. A constituição de uma capacidade de resposta a incidentes é essencial e deve existir, caso seja contratualizada é responsabilidade da organização orientar essa capacidade;

PP. 5 Estabelecer relações e ligações com organizações internas e externas e que estejam diretamente envolvidas na gestão de eventos, incidentes e vulnerabilidades;

PP. 6 Estabelecer e implementar os mecanismos técnicos, organizacionais e operacionais necessários para operacionalizar a atividade da CSIRT. Desenvolver e implementar os sistemas de informação necessários para apoiar a CSIRT, incluindo uma base de dados. Estes mecanismos e sistemas destinam-se a evitar a ocorrência de incidentes ou a probabilidade de ocorrerem. (e.g: *firewall*, anti-vírus, sistema de ticketing como o RT/RTIR [1] ou OTRS [2]);

PP. 7 Planear e desenvolver um programa de sensibilização e treino sobre eventos, incidentes e gestão de vulnerabilidades;

PP. 8 Testar o plano de gestão de incidentes, os processos e os procedimentos.

Concluindo esta fase, as organizações devem estar preparadas para gerir de forma adequada incidentes de cibersegurança.

4.2.2 Deteção e Participação

Esta fase envolve a deteção, através de informações associadas e relatórios sobre a ocorrência de eventos e a existência de vulnerabilidades, por meios manuais ou automatizados. A participação de eventos e de vulnerabilidades não significa que estes sejam considerados e classificados como incidentes e podem ser analisados posteriormente, se necessário. Para esta fase devem ser concretizadas as seguintes práticas:

Práticas

DP. 1 Monitorizar e recolher *logs* dos sistemas e da atividade da rede pelos quais a CSIRT é responsável;

DP. 2 Detetar e relatar a ocorrência de um evento ou a existência de uma vulnerabilidade, seja de forma manual ou de forma automática;

DP. 3 Recolher informações sobre um evento ou vulnerabilidade;

DP. 4 Dispor de informações sobre o que está a acontecer, um quadro situacional, de fontes de dados internas e externas, incluindo o tráfego dos sistemas e da rede, *logs* de atividade, *feeds* de notícias sobre a situação política, social ou atividades económicas que possam afetar a atividade do incidente, *feeds* externos de tendências de incidentes, novos vetores de ataque, indicadores, novas estratégias e tecnologias de mitigação;

DP. 5 Garantir que todas as práticas, resultados e decisões relacionadas sejam devidamente registadas para posterior análise;

[1] Consultar: https://bestpractical.com/rtir/; Acedido em 10-10-2018
[2] Consultar: https://community.otrs.com/; Acedido em 10-10-2018

DP. 6 Assegurar que as provas digitais sejam recolhidas e armazenadas de forma segura, e que a sua preservação seja segura e continuamente monitorizada, caso as provas sejam necessárias para um processo judicial ou ações disciplinares internas;

DP. 7 Garantir que é seguido um regime de controlo de alterações para rastrear eventos e vulnerabilidades e manter a base de dados atualizada;

DP. 8 Escalar, de acordo com as necessidades, durante o decurso desta fase, para posterior revisão ou decisões.

Todas as informações recolhidas referentes a um evento ou vulnerabilidade devem ser armazenadas na base de dados gerida pela CSIRT. As informações relatadas durante cada prática devem ser o mais completas possíveis. Isto ajudará nas avaliações, decisões e ações a serem tomadas.

4.2.3 Análise e Avaliação

Nesta fase é feita a avaliação das informações associadas com a ocorrência de eventos e a decisão de classificar um evento como incidente de cibersegurança. Uma vez que foi detetado e relatado um evento, devem ser concretizadas as seguintes práticas:

Práticas

AA. 1 Distribuir a responsabilidade pelas práticas de gestão de incidentes, através de uma cadeia hierárquica adequada, a pessoas que vão realizar a avaliação, tomada de decisão e as ações, envolvendo pessoas que poderão estar ou não relacionadas com a área de cibersegurança, se necessário;

AA. 2 Fornecer os procedimentos que cada pessoa notificada deve seguir, incluindo rever e corrigir relatórios, para avaliar os danos e notificar as pessoas relevantes. As ações individuais dependem do tipo e gravidade do incidente;

AA. 3 Utilizar diretrizes para documentar de forma completa um evento e as ações subsequentes para um incidente, se o evento for classificado como um incidente;

AA. 4 Recolher informações que podem incluir testes, medições e outros dados sobre a deteção de um evento. O tipo e a quantidade da informação recolhida dependerá do evento que ocorreu;

AA. 5 Levar a cabo uma avaliação, para determinar se o evento é um possível incidente ou um falso alarme. Um falso positivo é a indicação de um evento que foi detetado e relatado e que não constitui uma ameaça real ou não tem qualquer consequência. Tratando-se de um incidente, deve ser classificado segundo uma classe de incidente e tipo de incidente de acordo com a taxonomia em uso da RNCSIRT. Se necessário, a CSIRT pode rever a avaliação para se assegurar que o incidente foi declarado corretamente;

AA. 6 Assegurar que todas as partes envolvidas, em particular a CSIRT, registam todas as práticas, resultados e decisões para posterior análise;

AA. 7 Garantir que o registo de controlo de alterações é mantido de modo a rastrear os incidentes e as atualizações que vai recebendo num relatório do incidente, mantendo deste modo a respetiva base de dados atualizada.

Todas as informações recolhidas referentes a um evento, incidente ou vulnerabilidade devem ser armazenadas na base de dados gerida pela CSIRT. As informações comunicadas durante cada prática devem ser tão completas quanto possíveis no momento.

4.2.4 Resposta e Documentação

Esta fase envolve responder a incidentes de acordo com as ações determinadas na fase de análise e avaliação. Dependendo das decisões, as respostas podem ser feitas de forma imediata ou num curto espaço de tempo e em algumas pode ser necessário realizar uma investigação de segurança. Uma vez que um incidente foi confirmado e as respostas determinadas, devem ser concretizadas as seguintes práticas:

Práticas

RD. 1 Distribuir a responsabilidade pelas práticas de gestão de incidentes através de uma cadeia hierárquica adequada, a pessoas que têm de tomar decisões e ações, envolvendo pessoas que poderão estar ou não relacionadas com a área de cibersegurança, conforme necessário;

RD. 2 Fornecer os procedimentos que cada pessoa envolvida deve seguir, incluindo rever e alterar relatórios, reavaliar os danos e notificar as pessoas relevantes. As ações individuais dependem do tipo e da severidade do incidente;

RD. 3 Usar diretrizes para documentar de forma exaustiva um incidente e as ações subsequentes;

RD. 4 Investigar os incidentes de acordo e com a sua classificação. A classificação pode ser alterada se necessário. A investigação pode incluir diferentes tipos de análises para fornecer um entendimento mais profundo dos incidentes;

RD. 5 Determinar se o incidente está sob controlo e, em caso afirmativo, executar a resposta necessária. Se o incidente não está sob controlo ou vai ter um impacto grave sobre a atividade da organização, realizar práticas de resposta a crises através do escalonamento para a função de tratamento de crises;

RD. 6 Atribuir recursos internos e identificar recursos externos a fim de responder a um incidente;

RD. 7 Escalar conforme necessário ao longo da fase para futuras avaliações ou decisões;

RD. 8 Garantir que todas as partes envolvidas, em particular a CSIRT, registam todas as práticas para posterior análise;

RD. 9 Assegurar que as provas digitais são recolhidas e armazenadas de forma segura, e a sua preservação seja continuamente monitorizada, caso sejam necessárias para um processo judicial ou para ações disciplinares internas;

RD. 10 Garantir que o registo de controlo de alterações é mantido de modo a rastrear os incidentes e as atualizações que vai recebendo num relatório do incidente, mantendo deste modo a respetiva base de dados atualizada;

RD. 11 Comunicar a existência do incidente e partilhar detalhes relevantes (e.g: informações sobre ameaças, ataques e vulnerabilidades) com outros indivíduos ou organizações internas e externas, de acordo com as normas da organização e planos de comunicação e políticas de

divulgação de informações do CSIRT. Pode ser importante notificar os proprietários dos ativos (determinados durante a análise de impacto) e as organizações internas e externas (e.g: outras CSIRTs, Autoridades Nacionais - CNCS, PJ, fornecedores de serviços de Internet e outras organizações de uma comunidade) que poderiam ajudar na gestão e resolução do incidente.

Partilhar informações também pode beneficiar outras organizações, já que as mesmas ameaças e ataques geralmente afetam várias organizações. A partilha de informações deve ser efetuada de acordo com o estipulado no TLP;

RD. 12 Avaliar se após a recuperação de um incidente, deve ser iniciada uma análise após incidente, dependendo da natureza e gravidade. Esta prática inclui: investigação das informações relativas ao incidente, investigação de outras fontes relevantes, tais como o pessoal envolvido, e relatório dos resultados da investigação;

RD. 13 Elaborar um relatório final depois do incidente ter sido resolvido e encerrado, do qual todas as partes interessadas devem ser notificadas.

4.2.5 Lições Aprendidas

A fase das lições aprendidas ocorre quando os incidentes e as vulnerabilidades são resolvidos. Devem ser retiradas as aprendizagens de como os incidentes e as vulnerabilidades foram tratados. As lições aprendidas devem traduzir-se em melhorias ou alterações a efetuar e incorporar no planeamento e preparação. Para tal, devem ser concretizadas as seguintes práticas:

Práticas

LA. 1 Reconhecer quais foram as lições aprendidas a partir dos incidentes e das vulnerabilidades, devendo-se analisar exatamente o que aconteceu e em que momentos;

LA. 2 Identificar e otimizar a implementação de controlos de segurança, bem como a política de cibersegurança. Os contributos, para a implementação de novos controlos ou atualização de outros já em vigor, podem surgir de um ou vários incidentes ou de vulnerabilidades reportadas. As alterações a ocorrer têm de ser inseridas na estratégia da organização para se saber que investimentos são necessários;

LA. 3 Rever e melhorar a avaliação e gestão do risco existente na organização;

LA. 4 Verificar a eficiência dos processos, procedimentos, relatórios e da estrutura organizacional em responder, avaliar e recuperar de incidentes e lidar com vulnerabilidades. Baseados nas lições aprendidas, identificar e aperfeiçoar o plano de gestão de incidentes e a sua documentação;

LA. 5 Comunicar e partilhar os resultados da avaliação dentro de uma comunidade, caso a organização assim o pretenda;

LA. 6 Verificar se as informações sobre um incidente, vetores de ataque relacionados e vulnerabilidades podem ser partilhadas com outras organizações de uma comunidade, com as quais haja parcerias, com o objetivo de impedir que os mesmos incidentes se possam propagar a essas organizações. Esta partilha de informações deve ser efetuada de acordo com o estipulado no TLP;

LA. 7 Avaliar periodicamente o desempenho e a eficácia da CSIRT. A avaliação da maturidade pode ser feita segundo o modelo SIM3.

As práticas do processo de gestão de incidentes são iterativas. A organização deve introduzir melhorias ou correções onde sejam identificadas essas necessidades ao longo do tempo.

Com base na análise dos dados sobre incidentes e vulnerabilidades reportados e nas respostas que foram dadas aos incidentes, devem ser propostas alterações, tanto a elementos de segurança e às medidas que devem ser tomadas e implementadas, como ao próprio processo de gestão de incidentes.

Capítulo 5

Demonstração

Neste capítulo, descrevemos como foi efetuada a demonstração e aplicação do nosso processo de referência para gestão de incidentes de cibersegurança numa organização. Elegemos uma organização pública, de nome fictício DemoPub, que presta serviços na área da cibersegurança, caracterizada por ter uma CSIRT constituída e com maturidade na resposta a incidentes. Já tem o processo de gestão de incidentes de cibersegurança implementado e manifestou interesse em que este fosse avaliado por comparação com a solução ora apresentada.

5.1 Objetivo

O objetivo desta demonstração foi avaliar se o processo de gestão de incidentes, implementado e em utilização pela DemoPub, podia ser alvo de melhorias, tendo em conta o processo de referência proposto e baseado no trabalho desenvolvido nesta dissertação.

5.2 Auto-avaliação

Iniciámos a demonstração com o enquadramento e a apresentação da solução ao responsável pela CSIRT e um dos seus técnicos. Descrevemos a estrutura e o pretendido com as fases a realizar, correspondentes práticas e o que era esperado atingir em cada uma delas.

Começámos por verificar que dispunham de documentos que estabelecem o seu funcionamento e que estão de acordo com o considerado nas práticas da fase de Planeamento e Preparação. Dispõem de um manual escrito onde está definido todo o seu processo de gestão de incidentes com as políticas descritas e aplicadas, procedimentos a adotar e que sustentam a sua atividade.

Elaborámos tabelas comparativas, que apresentamos, de seguida, através de figuras, para cada uma das fases, e comparámos o que ”Consta” e ”Não Consta” em cada uma das práticas correspondentes e em cada um dos processos.

Realizámos uma iteração completa do processo de referência proposto, em simultâneo com a execução da gestão e tratamento de um incidente.
Para a fase de Planeamento e Preparação apresentam-se de seguida os resultados dessa comparação, traduzidos através da Figura 5.1

Fase: Planeamento e Preparação				
	Processo proposto		DemoPub	
Prática	Consta	Não consta	Consta	Não consta
PP. 1	X		X	
PP. 2	X		X	
PP. 3	X		X	
PP. 4	X		X	
PP. 5	X		X	
PP. 6	X		X	
PP. 7	X		X	
PP. 8	X		X	

Figura 5.1: Avaliação da fase Planeamento e Preparação

Identificámos de seguida a fase de Deteção e Participação e comparámos os resultados obtidos, que se concretizam na Figura 5.2.

Fase: Deteção e Participação				
	Processo proposto		DemoPub	
Prática	Consta	Não consta	Consta	Não consta
DP. 1	X		X	
DP. 2	X		X	
DP. 3	X		X	
DP. 4	X		X	
DP. 5	X		X	
DP. 6	X		X	
DP. 7	X		X	
DP. 8	X		X	

Figura 5.2: Avaliação da fase Deteção e Participação

Concluída esta fase, prosseguimos para a fase de Análise e Avaliação, apresentando-se através da Figura 5.3 os resultados da respetiva comparação.

Fase: Análise e Avaliação				
	Processo proposto		DemoPub	
Prática	Consta	Não consta	Consta	Não consta
AA. 1	X		X	
AA. 2	X		X	
AA. 3	X		X	
AA. 4	X		X	
AA. 5	X		X	
AA. 6	X		X	
AA. 7	X		X	
AA. 8	X		X	

Figura 5.3: Avaliação da fase Análise e Avaliação

Através da fase de Resposta e Documentação, e conforme indicado nos resultados comparativos que se apresentam na Figura 5.4, foi identificada uma prática que não se encontrava prevista no processo da DemoPub.

Fase: Resposta e Documentação				
	Processo proposto		DemoPub	
Prática	Consta	Não consta	Consta	Não consta
RD. 1	X		X	
RD. 2	X		X	
RD. 3	X		X	
RD. 4	X		X	
RD. 5	X		X	
RD. 6	X		X	
RD. 7	X		X	
RD. 8	X		X	
RD. 9	X		X	
RD. 10	X		X	
RD. 11	X		X	
RD. 12	X		X	
RD. 13	X			X

Figura 5.4: Avaliação da fase Resposta e Documentação

Finalizando esta iteração, apresentamos de seguida os resultados da comparação efetuada entre processos na fase das Lições Aprendidas, e traduzida através da Figura 5.5.

Fase: Lições Aprendidas				
	Processo proposto		DemoPub	
Prática	Consta	Não consta	Consta	Não consta
LA. 1	X		X	
LA. 2	X		X	
LA. 3	X		X	
LA. 4	X		X	
LA. 5	X		X	
LA. 6	X		X	
LA. 7	X		X	

Figura 5.5: Avaliação da fase Lições Aprendidas

Os resultados obtidos através desta Demonstração serão posteriormente avaliados no Capítulo 6.

Terminámos a demonstração e verificámos que o processo de gestão de incidentes que a DemoPub tem implementado já se encontra num nível de concretização elevado comparativamente ao processo de referência proposto.

Capítulo 6

Avaliação

Neste capítulo avaliamos o trabalho que desenvolvemos e verificamos se foi atingido o objetivo a que nos propusemos. Começamos por avaliar os resultados das entrevistas realizadas junto de dez especialistas em cibersegurança, seguidamente apresentamos os resultados obtidos da demonstração, que realizámos junto de uma organização e, finalmente, avaliamos se o artefacto que produzimos satisfaz as exigências previstas na metodologia de investigação utilizada.

6.1 Entrevistas

As entrevistas que foram realizadas tinham como objetivo recolher contributos para esta dissertação. Avaliando as respostas obtidas obtivemos e extraímos contributos e a partir deles conseguimos validar que a gestão de incidentes de cibersegurança tem de ser feita de forma metódica e estruturada. Que tem se ser vista de uma forma holística e transversal a toda a organização.

Com os contributos obtidos dos entrevistados e através da análise do conteúdo das suas respostas foi possível validar diversos pontos comuns nas fases da solução que apresentámos.

6.2 Demonstração

Através da avaliação da demonstração pretendemos verificar se o processo de referência proposto poderia trazer benefícios à organização onde fosse implementado. A demonstração, conforme referido no capítulo anterior, concretizou-se numa auto-avaliação realizada numa organização pública.

Mediante essa auto-avaliação, comparou-se o processo de gestão de incidentes de cibersegurança da organização com o processo proposto no âmbito desta dissertação. Os resultados obtidos concretizaram-se nas figuras que apresentámos no capítulo 5.

Avaliámos o processo em todas as suas fases, verificando individualmente e realizando as respetivas práticas. Nessas circunstâncias, foi identificada uma prática que o nosso processo prevê mas que não é contemplada pelo processo da DemoPub. Identificando-se neste ponto uma melhoria que deve ser implementada e que foi reconhecida como mais valia para o processo da organização. Mais concretamente, detetou-se que faltava preencher um relatório final de cada incidente, processo que não se encontrava devidamente endereçado pela DemoPub.

Apesar do processo de referência que apresentámos ser de alto nível, verificamos que um dos principais objetivos foi alcançado, resultando também daí que o processo de referência para gestão de incidentes de cibersegurança pode trazer benefícios e contribuir para melhorar a implementação de um processo já existente.

6.3 Artefacto

É referido na metodologia de investigação DS que é necessária a aplicação de práticas rigorosas na avaliação dos artefactos desenhados.

Para tal, propomos avaliar o artefacto de acordo com *Prat et al.* [49], recorrendo a uma hierarquia de critérios de avaliação para artefactos de sistemas de informação, organizados de acordo com as dimensões de um sistema e que são: o objetivo, o contexto, a estrutura, a atividade e a evolução. Para cada uma das referidas dimensões, foi definido um conjunto de critérios, detalhados em subcritérios. Selecionámos três critérios para avaliar o nosso artefacto.

Escolhemos os critérios:

- contexto - consistência com as pessoas - fácil utilização;
- contexto - consistência com a organização - utilidade;
- estrutura - nível de detalhe.

Estes critérios foram considerados os mais adequados à nossa pesquisa e referidos como relevantes por *Hevner et al.* [1]. Justificamos essa escolha pelos seguintes motivos:

Contexto - consistência com as pessoas - fácil utilização: a solução fornece uma objetividade clara do que se pretende. O facto de estar escrita na língua portuguesa torna-se mais fácil de perceber e de utilizar;

Contexto - consistência com a organização - utilidade: a solução foi criada para organizações. Dá resposta a um problema que foi identificado e demonstrado na prática, por isso a sua utilidade fica justificada;

Estrutura - nível de detalhe: a solução apresenta um nível de detalhe considerado adequado e sistematizado, de carácter abrangente e de alto nível.

Estando o artefacto suportado e alinhado com uma norma internacional podemos considerá-lo como válido para atingir o objetivo proposto. Uma organização que adote e faça o alinhamento pela norma ISO/IEC 27035 fica preparada para no futuro realizar a certificação na norma ISO/IEC 27001.

Em resumo, e finalizando esta avaliação podemos concluir que o artefacto atinge o objetivo a que nos propusemos e contribui para a implementação do processo de gestão de incidentes de cibersegurança nas organizações portuguesas.

Capítulo 7

Conclusão

Apresentamos agora as conclusões retiradas da realização desta dissertação, referindo os contributos e indicando as limitações encontradas, bem como propostas de desenvolvimento em trabalho futuro. A realização deste trabalho de investigação teve como objetivo a definição de um método, que também designámos por processo de referência, para a gestão de incidentes de cibersegurança.

Pelos resultados da avaliação concluímos que o artefacto criado pode contribuir para resolver o problema da insuficiente preparação das organizações portuguesas para gerir incidentes de cibersegurança, cumprindo assim o objetivo a que nos propusemos.

A gestão de incidentes de cibersegurança deve ser realizada pela necessidade de garantir a segurança da informação, segundo refere D. Santos [12]. Sem essa garantia de segurança podem vir a ser postas em causa funções essenciais na sociedade.

Os ativos de qualquer organização são as pessoas, os dados e os processos. Se algum dos três for comprometido os restantes irão ser afetados. Relevamos a importância da inventariação de todos os ativos, a sua proteção e defesa adequadas.

A gestão de incidentes de cibersegurança não é só uma questão técnica e deve ser abordada de forma preventiva e não só reativa. Também deve ser vista como parte de um processo global e integrante da organização. Ser encarada como um percurso que se constrói com capacidade e maturidade e que adiciona valor, envolvendo a organização como um todo, e ter o comprometimento e a sua sustentação pela gestão de topo.

Podemos concluir que existem algumas organizações públicas com um elevado nível de maturidade na gestão de incidentes de cibersegurança, possuindo um processo de gestão de incidentes já implementado e documentado. Por outro lado, identificámos pelas entrevistas, que existem organizações que se encontram a iniciar o seu processo e outras que não possuem nada definido.

Em resposta à questão que levantámos no problema concluímos que as organizações portuguesas, públicas e privadas, ainda não se encontram suficientemente preparadas para gerir este tipo de incidentes. É, pois, necessário percorrer um longo percurso de adaptação e transformação devendo as organizações capacitarem-se nesta área [50].

Concluímos que o elo mais fraco será o ser humano e que os incidentes de cibersegurança são

essencialmente causados por comportamentos inadequados dos utilizadores. O caminho passa por desenvolver planos de formação e treino adaptados a todos os colaboradores.

Podemos igualmente concluir que a adoção de um normativo internacional reconhecido, como foi neste caso concreto a ISO/IEC 27035, tem vantagens ao nível da harmonização e interoperabilidade.

A possibilidade que nos foi concedida para realizarmos a demonstração da nossa solução, permitiu ainda verificar o processo de gestão e resposta a incidentes e, com isso, compreender o seu processamento e o trabalho prévio que é necessário fazer.

7.1 Contributos

Para gerir incidentes de cibersegurança devem ser seguidas as diretrizes presentes na ISO/IEC 27035. A adoção desta norma, que complementa outras normas existentes, permite que no futuro se possa fazer a certificação no âmbito da ISO/IEC 27001.

Refiram-se ainda, como contributo adicional, algumas das causas identificadas sobre a insuficiente preparação das organizações: o reajuste orgânico na estrutura das organizações públicas, fusões ou separação de organismos; a falta de inventariação e identificação de todos os ativos; a falta de recursos humanos, sua formação e capacitação; as limitações das organizações públicas ao nível da contratação pública e da gestão de orçamentos; dificuldades no acesso a formação; a ausência de políticas e procedimentos; os investimentos feitos aos quais não é retirado proveito.

Finalmente, considera-se que o trabalho de pesquisa que foi desenvolvido no âmbito desta dissertação deverá ser considerado como contributo e desse modo adicionado à *Knowlegde Base*, conforme referido no final da Metodologia de Investigação da *Design Science*.

7.2 Limitações

A conclusão desta dissertação sofreu alguns contratempos devido a ter sido necessário reajustar a metodologia de investigação, por se entender que a *Design Science* seria a mais adequada ao problema.

O artefacto produzido traduz um método de alto nível que carece de maior detalhe em desenvolvimentos futuros.

A implementação desta solução, numa organização que esteja a iniciar a implementação do processo de gestão de incidentes de cibersegurança, pode ser demorada no tempo devido aos requisitos necessários.

A quantidade de itens que a norma ISO/IEC 27035 apresenta é extensa, sendo necessário que cada organização faça uma adaptação à sua realidade e dimensão.

7.3 Trabalho Futuro

Como trabalho futuro propomos o desenvolvimento do método no que diz respeito aos seus procedimentos e *guidelines* necessários a cada uma das suas fases, bem como o desenho de *workflows*.

Ainda como trabalho futuro propomos o desenvolvimento de relatórios para participação de incidentes às autoridades portuguesas.

Como proposta final entendemos que seria interessante implementar a solução na sua completude numa organização e fazer o seu acompanhamento do princípio ao fim.

Por fim, refira-se que seguimos e cumprimos as diretrizes apresentadas na metodologia de investigação e com isso damos este trabalho de pesquisa por concluído.

Bibliografia

[1] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, pp. 75–105, Mar. 2004. https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research, Acedido em 28-08-2018.

[2] ENISA, "Good Practice Guide for Incident Management." https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management, Acedido em 15-12-2017.

[3] Comissão Europeia, "Estado da União 2017 – Cibersegurança: Comissão reforça a resposta da UE aos ciberataques," Maio 2017. http://europa.eu/rapid/press-release_IP-17-3193_pt.pdf, Acedido em 02-01-2018.

[4] Centro Nacional de Cibersegurança, "Glossário." https://www.cncs.gov.pt/recursos/glossario/, Acedido em 23-09-2018.

[5] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical," Abril 2017. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010, Acedido em 17-09-2018.

[6] A. Morse, "Investigation: WannaCry cyber attack and the NHS," Report HC 414 SESSION 2017–2019, National Audit Office, Apr. 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, Acedido em 24-12-2017.

[7] SapoTek, "Cibersegurança: Cooperação entre diferentes entidades é obrigatória para enfrentar os riscos crescentes." https://tek.sapo.pt/noticias/computadores/artigos /ciberseguranca-cooperacao-entre-diferentes-entidades-e-obrigatoria-para-enfrentar-os-riscos-crescentes, Junho 2017. Acedido em 09-08-2018.

[8] U.S. Departement of Commerce, NIST - National Institute of Standards and Technology, *Computer Security Incident Handling Guide*. NIST, Agosto 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Acedido em 26-08-2018.

[9] Sistema de Segurança Interna, "Relatório Anual de Segurança Interna 2017." https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6, Acedido em 06-06-2018.

[10] Banco de Portugal, "Intervenção na sessão de abertura do Administrador Hélder Rosalino na Conferência Cibersegurança no sistema financeiro: riscos, cooperação e governação," Junho 2017. https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20170630.pdf, Acedido em 02-01-2018.

[11] Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas (INA), "Ciberhigiene: Glossário." https://moodle.ina.pt/mod/page/view.php?id=4707%5C, Acedido em 13-09-2018.

[12] D. Santos, "A Cibersegurança em Portugal: a ação política nacional em matéria de cibersegurança," Master's thesis, ISCTE-IUL, 2014. http://hdl.handle.net/10071/8844, Acedido em 29-08-2018.

[13] National Initiative for Cybersecurity Careers and Studies, "Glossary." https://niccs.us-cert.gov/about-niccs/glossary, Acedido em 23-09-2018.

[14] Parlamento Europeu e Conselho da União Europeia, "Diretiva (UE) 2016/1148, de 6 de julho," Julho 2016. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.POR&toc=OJ:L:2016:194:TOC, Acedido em 20-08-2018.

[15] Assembleia da República, "Lei n.º 46/2018 - Regime Jurídico de Segurança do Ciberespaço," Agosto 2018. http://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html, Acedido em 13-08-2018.

[16] Rede Nacional CSIRT, "Rede Nacional CSIRT." http://www.redecsirt.pt/#docs, Acedido em 13-09-2018.

[17] Assembleia da República, "Lei n.º 109/2009, Lei do Cibercrime." https://dre.pt/application/conteudo/489693, Acedido em 20-08-2018.

[18] L. Santos, "Contributos para uma melhor governança da cibersegurança em Portugal," Master's thesis, Faculdade de Direito da Universidade Nova de Lisboa, 2011. http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF, Acedido em 02-09-2018.

[19] Direção-geral da Administração e do Emprego Público, "Organização da administração do estado." https://www.dgaep.gov.pt/index.cfm?OBJID=a5de6f93-bfb3-4bfc-87a2-4a7292719839&men=i, Acedido em 19-08-2018.

[20] H. Bronk, M. Thorbruegge, and M. Hakkaja, "A step-by-step approach on how to set up a csirt." https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport/CSIRT_setting_up_guide_ENISA.pdf, Acedido em 12-08-2018.

[21] Comissão Europeia, "COM(2017) 476 - Comunicação da Comissão ao Parlamento Europeu e ao Conselho." https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-476-F1-PT-MAIN-PART-1.PDF, Acedido em 02-01-2018.

[22] Comissão Europeia, "Anexo da Comunicação da Comissão ao Parlamento Europeu e ao Conselho." https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0476&qid=1538255134349&from=EN, Acedido em 02-01-2018.

[23] Presidência e da Modernização Administrativa, "Decreto-Lei n.º 136/2017, de 6 de novembro - Altera a orgânica do Gabinete Nacional de Segurança." http://data.dre.pt/eli/dec-lei/136/2017/11/06/p/dre/pt/html, Acedido em 15-09-2018.

[24] Conselho da União Europeia, Parlamento Europeu, "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, (Regulamento Geral sobre a Proteção de Dados)." https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt, Acedido em 02-09-2018.

[25] Assembleia da República, "Lei n.º 26/2016, de 22 de agosto." http://data.dre.pt/eli/lei/26/2016/08/22/p/dre/pt/html, Acedido em 02-09-2018.

[26] Presidência do Conselho de Ministros, "Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho - Estratégia Nacional de Segurança do Ciberespaço." http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html, Acedido em 02-09-2018.

[27] C. Hove, M. Tarnes, M. Bartnes, and K. Bernsmed, "Information security incident management: Identified practice in large organizations," in *Proceedings - 8th International Conference on IT Security Incident Management and IT Forensics, IMF 2014*, pp. 27–46, 05 2014.

[28] ISO/IEC, "Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management," International Standard ISO/IEC 27035-1:2016, International Organization for Standardization/International Electrotechnical Commission, November 2016.

[29] ISO/IEC, "Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response," International Standard ISO/IEC 27035:2016, International Organization for Standardization/International Electrotechnical Commission, October 2016.

[30] BMC, "ITIL Incident Management." http://www.bmcsoftware.pt/guides/itil-incident-management.html#, Acedido em 23-05-2018.

[31] P. Kral, "The Incident Handlers Handbook." https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901, Acedido em 01-02-2018.

[32] Centro Nacional de Cibersegurança, "Modelo de Maturidade de Reação." https://www.cncs.gov.pt/content/files/modelomaturidadereacao_201708.pdf, Acedido em 01-02-2018.

[33] ENISA, "Reference Incident Classification Taxonomy." https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/at_download/fullReport/WP2017O-3-1-1GoodpracticeguideonhowtoimproveCSIRTcapabilities.pdf, Acedido em 01-09-2018.

[34] Europol, "Common Taxonomy for Law Enforcement and The National Network of CSIRTs." https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf, Acedido em 20-08-2018.

[35] FIRST, "TRAFFIC LIGHT PROTOCOL (TLP)." https://www.first.org/tlp/, Acedido em 01-09-2018.

[36] ENISA, "Considerations on the Traffic Light Protocol." https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol, Acedido em 01-09-2018.

[37] D. Stikvoort, "Trusted-Introducer:Processes:Certification." https://www.trusted-introducer.org/SIM3-Reference-Model.pdf, Acedido em 01-08-2018.

[38] ENISA, "CSIRT Maturity - Self-assessment Survey." https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey, Acedido em 01-08-2018.

[39] P. Green, "Itil." http://www.isaca.org/Groups/Professional-English/itil/Pages/ViewDiscussion.aspx?PostID=136, Acedido em 02-01-2018.

[40] P. Bernard, *Foundations of ITIL 2011 Edition*. Van Haren Publishing, 2012.

[41] R. Pereira and M. M. da Silva, "A maturity model for implementing itil v3 in practice," in *2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops*, pp. 259–268, Aug 2011.

[42] ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT." http://www.isaca.org/COBIT/Pages/default.aspx, Acedido em 23-05-2018.

[43] IT Governance Institute, *Cobit 4.1*. ISACA, 2007.

[44] ISACA, "DS5.6 - Security Incident Definition." https://www.isaca.org/Groups/Professional-English/ds5-6-security-incident-definition/Pages/Overview.aspx, Acedido em 03-01-2018.

[45] ISACA, *COBIT 5: Enabling Processes*. ISACA, 2012.

[46] ISO/IEC, "Information technology – Security techniques – Code of practice for information security controls," International Standard ISO/IEC 27002:2013, International Organization for Standardization/International Electrotechnical Commission, October 2013.

[47] International Organization for Standardization (ISO), "ISO/IEC 27001 Information security management." https://www.iso.org/isoiec-27001-information-security.html, Acedido em 1-10-2018.

[48] ISO/IEC, "Information technology – Security techniques – Information security management systems — Requirements," International Standard ISO/IEC 27001:2013, International Organization for Standardization/International Electrotechnical Commission, October 2013.

[49] N. Prat, I. Wattiau, and J. Akoka, "Artifact Evaluation in Information Systems Design Science Research - A Holistic View," *PACIS 2014 Proceedings. 23*, 2014.

[50] Computerworld, "Preparar os trabalhadores para a cibersegurança." https://static.computerworld.com.pt/media/2018/01/CW_janeiro_2018-preparar-os-trabalhadores-para-a-cibersegurança.pdf, Janeiro 2018. Acedido em 12-08-2018.

Apêndice A

Anexo A

TÉCNICO LISBOA

Investigador: Daniel Matos (daniel.matos@tecnico.ulisboa.pt)

Guia da Entrevista

Este estudo é parte de uma pesquisa intitulada "Gestão de incidentes de cibersegurança em Organizações Públicas" no âmbito do Mestrado em Engenharia Informática e de Computadores do Instituto Superior Técnico (IST), desenvolvido pelo estudante Daniel Matos, sob a supervisão do Professor Miguel Mira da Silva (IST) e do Eng. Nuno Fernandes (CNCS).

Enquadramento: A insuficiente preparação das organizações para lidar com ciberataques cada vez mais sofisticados é reconhecida publicamente.

Objetivo: O objetivo desta entrevista é identificar as causas da insuficiente preparação das organizações para lidar com ciberataques cada vez mais sofisticados, com base na experiência e conhecimento de profissionais da área.

O questionário está dividido em duas secções:

1. Questões relacionadas com a sua formação e experiência enquanto profissional de Tecnologias de Informação (TI).

2. Questões relacionadas com incidentes de cibersegurança.

Termos Gerais

- O tempo da entrevista é de aproximadamente trinta minutos. Se consentir pretendo gravar a entrevista. Sinta-se à vontade para interromper a qualquer momento.
- Este estudo será dirigido a profissionais de TI de diferentes organizações.
- Os resultados deste estudo poderão ser submetidos a conferências e revistas académicas.
- O propósito desta entrevista é somente académico, as informações pessoais e da sua organização serão protegidas mantendo a sua confidencialidade.

Questionário Gestão de Incidentes de Cibersegurança em Organizações Públicas

Secção 1 - Informação Pessoal

Das questões que se seguem, selecione as opções que se adequam ao seu caso:

1. Nível escolaridade:

- ◯ 12º Ano
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Outro (indique qual)

2. Cargo/Função atual:

- ◯ Técnico de Informática
- ◯ Especialista de Informática
- ◯ Consultor
- ◯ Chefia Intermédia
- ◯ Direção de Serviço
- ◯ CIO
- ◯ CEO
- ◯ CTO
- ◯ CISO
- ◯ Outro (indique qual)

3. Experiência em TI área Segurança/Cibersegurança (anos):

- ◯ Menos de 5
- ◯ Entre 5 e 10
- ◯ Entre 10 e 15
- ◯ Entre 15 e 20
- ◯ Mais de 20

4. Exerce funções no Sector:

◯ Público ◯ Privado

Secção 2 - Gestão de Incidentes de Cibersegurança

1. O que entende por incidente de cibersegurança?

2. Os incidentes de cibersegurança, no seu entender, são essencialmente causados por questões técnicas ou por questões comportamentais? Justifique.

3. Entende que deve existir uma política de cibersegurança transversal suportada e aprovada pelo órgão máximo da organização? Na sua organização existe e é aplicada? Se aplicável, quem a aprovou?

4. Considera que a inventariação e gestão dos ativos e serviços críticos podem contribuir para reduzir a exposição a incidentes de cibersegurança? Realizam essa inventariação e gestão de forma contínua e está atualizada?

5. Quer indicar uma ou mais normas ou guias para a gestão de incidentes de cibersegurança que conheça? Caso tenha indicado alguma(s), a(s) mesma(s) é(são) aplicada(s) na organização?

6. Faz sentido existir uma harmonização na utilização de boas práticas e normas nacionais/internacionais na forma de gerir este tipo de incidentes? Se sim, quais as que utilizam? Se não, justifique a sua resposta.?

7. A gestão e tratamento dos incidentes de cibersegurança deve seguir uma metodologia própria e bem definida ou pode ser ad-hoc? No caso da sua organização, qual é a abordagem utilizada?

8. A existência de uma equipa de resposta a incidentes de cibersegurança deve ter definidas as suas competências e atribuições. O mandato deve ser dado pelo topo da organização ou pelo departamento responsável pela área de TI? Justifique a sua resposta.

9. O treino e a preparação da equipa de resposta a incidentes deve ser encarada como uma mais valia para a organização ou como um custo? Se a sua organização dispõe desta equipa, como é que é encarada? Se não tem ninguém dedicado, quais são as razões para

não ter?

10. Tendo sido detetado um incidente, considera que deve existir uma análise detalhada para saber o que aconteceu e criar conhecimento interno para aprender e evitar situações futuras? Isso é aplicado na sua organização? Se sim, de que forma?

A entrevista termina aqui.

As questões apresentadas merecem-lhe algum comentário ou deveria ter questionado algo que não foi mencionado?

Obrigado pela colaboração.

Data