O FATOR HUMANO NA CIBERSEGURANÇA

ISABEL MARGARIDA AFONSO DA SILVA BAPTISTA

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

Orientador: Professor Doutor Carlos Ribeiro

Co-orientador: Professor Doutor Pedro Veiga

Júri

Professor Doutor Paulo Mateus

Professor Doutor Carlos Ribeiro

Contra-Almirante António Gameiro Marques

Lisboa, 31 outubro de 2017

Agradecimentos

Esta dissertação deve a sua existência, apoio e inspiração a várias pessoas.

Ao Professor Doutor Carlos Ribeiro, por se ter disponibilizado para orientar este trabalho e pelo interesse demonstrado no tema tratado nesta dissertação.

Ao Professor Doutor Pedro Veiga, co-orientador desta dissertação, mentor e tutor profissional, o impulso, o estímulo e posterior apoio e disponibilidade demonstrados em todas as fases que levaram ao culminar desta fase do projeto.

Ao Professor Doutor Carlos Caleiro, professor e responsável por este mestrado no IST, pelo acompanhamento e disponibilidade em responder e clarificar todas as questões que foram ocorrendo ao longo dos últimos dois anos.

Ao Contra-Almirante António Gameiro Marques, pela confiança e contributo para a valorização pessoal e profissional, através da realização deste Mestrado e posterior apoio na realização este trabalho.

Ao Major Rogério Raposo e ao Eng. Lino Santos, meus bons amigos, pelo estímulo, sapientes sugestões, conhecimentos, disponibilidade e paciência.

Ao Gabinete Nacional de Segurança e Centro Nacional de Cibersegurança através dos colegas de trabalho, pela sua permanente amizade, espírito de equipa e contributos para estas temáticas e aos meus colegas do Gabinete do Coordenador pelo apoio, companheirismo e amizade

Aos responsáveis pelas entidades que participaram neste projeto, cuja disponibilidade e informações ajudaram à realização e enriquecimento deste projeto, especificamente ao Major Poiares da Guarda Nacional Republicana, ao Eng. Nuno Miranda do Instituto de Informática de Segurança Social, ao Dr. Rui Ribeiro da Fundação para a Computação Científica Nacional, à Dra. Lígia Azevedo da Direção Geral de Educação e à Dra. Sofia Rasgado da Fundação para a Ciência e Tecnologia.

À Aline e ao Norberto pelo apoio incondicional e por todas as ajudas do Mundo, pois sem elas tudo seria muito mais difícil.

À Filipa e ao Pedro pela paciência, apoio incondicional e contributos em áreas tão díspares, mas tão sensatas que se revelaram fundamentais.

Ao Gustavo, meu porto seguro, simplesmente por tudo.

Resumo

Face aos desafios tecnológicos diários e à necessidade de usar a Internet e as Tecnologias de informação e Comunicação (TIC), começam a ser percetíveis os profundos efeitos que estas tecnologias têm na sociedade contemporânea. Indivíduos, organizações e Estado, necessitam e dependem das TIC para as suas operações mais comuns ou triviais.

O constante desenvolvimento de novas ameaças e a abundância de ataques na Internet, exigem que o cidadão esteja mais consciente da relevância da proteção da sua informação e da sua identidade digital e esteja capacitado para se proteger.

Desconhecimento e falta de consciência em relação ao digital são as maiores ameaças aos sistemas de informação. Hoje que a segurança da informação, não depende somente de soluções técnicas, mas também do aumento da consciência e do adequado comportamento dos indivíduos na utilização dos sistemas de informação. As práticas comuns de segurança digital continuam a ser ignoradas pela generalidade dos indivíduos, pondo em risco não só a segurança dos seus dados e informação, mas a de todos os que os rodeiam. No entanto, a dimensão das consequências destas práticas de segurança, depende do entendimento claro sobre os riscos aos quais a informação está sujeita.

Tendo em conta a realidade descrita, considera-se fundamental contribuir para o despertar da consciencialização em cibersegurança, sendo este o ponto de partida para o desenvolvimento de um programa de capacitação de cidadãos em cibersegurança.

São apresentadas um conjunto de propostas que contribuem para o desenvolvimento de conteúdos de sensibilização e de capacitação das boas práticas de ciber-higiene.

Palavras-chave: *Cibersegurança, Sensibilização, Capacitação, ciber-higiene, desafios digitais, cibercidadão*

Abstract

Given the technological challenges we face daily and the need to use the Internet and Information and Communication Technologies (ICT) in daily tasks, the profound effects that these technologies have on contemporary society are beginning to be perceived. Individuals, organizations and the State need and depend on the Internet and ICT for their most common or trivial operations.

The constant emergence of new threats and the high number of attacks on the Internet require that citizens are aware of the importance of protecting their information, their digital identity, and being alert and capable of protecting themselves.

Ignorance and lack of awareness about digital challenges are the biggest threats to information systems. It is now known that information security depends not only on technical solutions, but also on increasing the awareness and appropriate behaviour of individuals in the use of information systems. Common digital security practices continue to be ignored by most individuals, jeopardizing not only the security of their data and information, but the safety of everyone around them. However, the scale of the consequences of these security practices depends on the clear understanding of the risks to which the information is subject.

Taking into account the reality described above, it is considered fundamental to contribute to the awakening of awareness in cybersecurity, which is the starting point for the development of a cybersecurity citizenship training program.

In this sense, a set of proposals are presented that contribute to the development of awareness and training contents of good cyber-hygiene practices.

Keywords: *Cybersecurity***,** *Awareness, Training, Cyber hygiene, digital challenges, cyber citizen*

Índice

Agradecimentos 3
Resumo 4
Abstract 5
Índice de Figuras 8
Acrónimos e Siglas 10
1. Introdução 12
1.1. Enquadramento 12
1.2. O problema 14
1.3. A missão do Centro Nacional de Cibersegurança 16
1.4. O papel da Estratégia Nacional de Segurança do Ciberespaço 17
1.5. Iniciativa Portugal INCoDe.2030 18
2. Educação, formação e capacitação 20
2.1. Educação e formação 22
2.2. Formação e capacitação 23
2.2.1. Formação em Cibersegurança 23
2.2.2. Capacitação 24
3. Principais programas de capacitação em cibersegurança 26
3.1. Na Europa 26
3.2. Nos Estados Unidos da América 28
3.3. Em Portugal 30
4. Políticas Públicas em Cibersegurança 40
4.1. Estratégia Nacional de Segurança do Ciberespaço (ENSC) 40
4.2. InCode2030 42
4.3. SIMPLEX + ... 44
4.4. Estado da União 2017 45
5. Programa de capacitação de cidadãos em cibersegurança 48
5.1. Planear, desenvolver e implementar um programa de capacitação em cibersegurança 49
5.1.1. Planear 49

5.1.2. Desenvolver 49
5.1.3. Implementar 49
5.1.4. Após implementar 50
5.1.5. Acompanhar a conformidade 50
5.1.6. Avaliação e *Feedback* 51
5.1.7. Gerir a mudança 51
5.1.8. Indicadores de sucesso do programa 51
5.2. O E-Learning e a cibersegurança 52
5.3. Os MOOC e a Cibersegurança 55
5.3.1. A certificação dos MOOC 57
5.4. Desenvolver o Programa de Capacitação em Cibersegurança para Cidadãos 59
5.5. Avaliação 66
6. Conclusão e trabalho futuro 68
6.1. Conclusão 68
6.2. Trabalho futuro 71
Bibliografia e Referências 72

Índice de Figuras

Figura 1 – Construção de uma carreira de cibersegurança 30
Figura 2 – Dados de Cibercrimes relativos aos anos 2014, 2015 e 2016 34
Figura 3 – Desenho estratégico do projeto Safer Internet - CyberGNRation 35
Figura 4 –Curso de E-Learning – Segurança na ponta dos dedos do II, I.P 38
Figura 5 - Dados relativos a crimes informáticos 39
Figura 6 - Eixos de atuação, princípios e objetivos da ENSC. 41
Figura 7 - The Digital Economy and Society Index (DESI) - DESI2017 43
Figura 8 - Resultado gráfico do Survey 2016 Report- Marsh 46
Figura 9 - Catálogo de cursos do MNE, destacando o curso de Segurança da informação – Matérias classificadas 2017 63
Figura 10 – Enquadramento do curso de capacitação de cidadãos em cibersegurança 64

Índice de Tabelas

Tabela 1- Dimensões de um MOOC (adaptado de Jansen & Schuwer, 2015) 55

Tabela 2- Exemplo de estrutura e organização de cursos MOOC (Porto, 2015)..... 59

Tabela 3- Tabela das Dimensões em Cibersegurança 61

Acrónimos e Siglas

ANNSI - Agence Nationale de la Sécurité des Systèmes d'Information

CE – Comissão Europeia

CEF - Connecting Europe Facility

CESG – National Technical Authority for Information Assurance

CIO – Chief Information Officer

CISO - Chief Information Security Officer

CNCS – Centro Nacional de Cibersegurança

CNPD - Comissão Nacional de Proteção de Dados

DGE – Direção Geral de Educação

DESI - Digital Economy and Society Index

DGIDC-CRIE - Direção Geral de Inovação e Desenvolvimento Curricular - Equipa de Missão Computadores, Redes e Internet

ENSC – Estratégia Nacional de Segurança do Ciberespaço

ENISA – European Network and Information Security Agency

EU - União Europeia

EUA – Estados Unidos da América

FAQ - Frequently Asked Questions

FCCN - Fundação para a Computação Científica Nacional

FCT - Fundação para a Ciência e Tecnologia

GCHQ - Government Communications Headquarters

GNR – Guarda Nacional Republicana

GNS – Gabinete Nacional de Segurança

IASME - Information Assurance Standard

IC – Infraestrutura Crítica

IISP - Information Security Skills Framework

IISS – Instituto de Informática da Segurança Social

IPDJ - Instituto Português do Desporto e Juventude

ISACA - Information Systems Audit and Control Association

ISF - Information Security Forum

ISO/IEC – International Organization for Standardization/ International Electrotechnical Commission

LMS - Learning Management System

MNE – Ministério dos Negócios Estrangeiros

NICE - National Initiative for Cybersecurity Education

NIST – National Institute of Standards and Technology

PME – Pequena e Média Empresa

PPP – Parceria Público-Privada

PT CIS – Centro Português de Internet Segura

SCADA/ICS - Supervisory control and data acquisition / Industrial Control Systems

TIC – Tecnologias da Informação e Comunicação

TI – Tecnologias de informação

1. Introdução

1.1. Enquadramento

Os rápidos avanços nas tecnologias da informação e da comunicação (TIC) têm um profundo efeito na sociedade contemporânea. Atualmente, indivíduos, organizações e Estado, necessitam da Internet e das TIC em geral para realizar tarefas diárias, o que significa que, genericamente, a sociedade e os indivíduos estão cada vez mais dependentes da tecnologia.

Os indivíduos dependem das TIC na sua vida quotidiana, resultando numa quase omnipresente adoção de tecnologia digital. Referindo apenas alguns exemplos, o indivíduo utiliza sistemas de informação para desempenhar as suas funções profissionais, joga em consolas de jogos e assiste a filmes em *tablets* para se entreter, utiliza recursos *on-line* para estudar, efetua compras na internet, interage e efetua consultas na internet através de *smartphones*, verifica as calorias consumidas e as horas dormidas através de sensores colocados nos pulsos, entre muitos outros.

Os sistemas de informação são, assim, fundamentais para o sucesso da Sociedade de Informação - uma sociedade globalizada, onde predomina a partilha e o simples e fácil acesso à informação.

O constante desenvolvimento de novas ameaças (com predominância no *malware*[1]); a abundância de ataques na Internet, como são o furto de dados, tais como fotografias, lista de contactos ou informações bancárias; o roubo de identidade ou o crime de extorsão, sendo o mais vulgar o *ramsomware*[2], exigem que o cidadão seja cada vez mais consciente da importância da proteção da sua informação e seja experiente e atento nessa proteção.

Apatia, ignorância ou não consciência em relação à segurança e iliteracia tecnológica são as maiores ameaças aos sistemas de informação. Sabe-se hoje que a melhor forma de obter uma melhoria significativa e perdurável no tempo, da segurança da informação, não é apenas através de soluções técnicas, mas também através do aumento da consciência e do adequado comportamento dos indivíduos na utilização dos sistemas de informação. O que deveriam ser práticas comuns de segurança digital continuam a ser ignoradas pela generalidade dos indivíduos, incluindo pelos indivíduos jovens que nasceram e cresceram com a tecnologia, pondo em risco não só a segurança dos seus dados e informação (incluindo a sua privacidade), mas a de todos os que os rodeiam.

No entanto, o alcance das consequências destas práticas de segurança também depende do entendimento claro e completo dos riscos aos quais a informação pode estar sujeita. A consciencialização é o ponto de partida para o desenvolvimento de um programa de capacitação de cidadãos, em cibersegurança, bem-sucedido.

---

[1] *Malware* (*malicous software*) é um *software* destinado a infiltrar-se num sistema de informático alheio de forma ilícita, com o objetivo de causar danos ou roubo de informações

[2] *Ransomware* é um tipo de *software* malicioso criado com o intuito de bloquear o acesso a ficheiros ou sistemas, cifrando-os, que só serão libertados após o pagamento de determinado valor. É como se fosse um sequestro, mas virtual.

O papel crítico que a consciência desempenha no ambiente organizacional tem sido amplamente defendido na literatura de Garantia da Informação (Hewitt, 2013). As organizações utilizam de forma massiva sistemas de informação, ligados a redes internas e à internet, dentro e fora do perímetro da infraestrutura da própria organização. Simplificando, com o aumento da conectividade, o risco de ataque às redes das organizações também aumenta.

Ao abordar o assunto da segurança da informação, existem três questões que influenciam a necessidade de um programa de capacitação de cidadãos para a Cibersegurança, onde se destaca a preservação da confidencialidade, da integridade, da disponibilidade e do não repúdio. Afirma-se que a informação está segura quando estas três propriedades estão presentes. Sendo um dos objetivos primordiais minimizar o risco associado ao uso das tecnologias digitais, abordando os dois componentes do risco - ameaças e vulnerabilidades, este trabalho sobre programas de capacitação incidirá na componente da redução do risco, nomeadamente, para proteger a confidencialidade, integridade e/ou disponibilidade dos sistemas de informação das organizações.

Tendo em conta a realidade descrita, considera-se assim fundamental contribuir para o despertar da consciencialização em cibersegurança.

Posto isto, o presente trabalho foca-se no desenho e desenvolvimento de um programa de capacitação de cidadãos em cibersegurança, nomeadamente no desenvolvimento de conteúdos de sensibilização, capacitação e respetivas métricas de avaliação para as boas práticas de utilização segura, consciente e mensurável dos recursos tecnológicos.

Na elaboração do presente trabalho foram observados e analisados vários programas prominentes de capacitação em cibersegurança, nomeadamente os desenvolvidos por outros Centros Nacionais de Cibersegurança ou organizações ligadas à sensibilização destas temáticas. O Centro Nacional de Cibersegurança (CNCS) considera que é condição essencial do apoio na proteção da confidencialidade, da integridade e da disponibilidade da informação dos organismos do Estado ou das Infraestruturas críticas (IC), a garantia de que cada indivíduo envolvido perceba as suas responsabilidades dentro da organização e na própria sociedade da informação, e esteja suficientemente preparado para o desempenho das suas funções em segurança.

O Capítulo II apresentará factos que revelam a tomada de consciência por parte das organizações relativamente à necessidade de competências em cibersegurança por parte das empresas. Neste sentido são apresentadas as mais relevantes distinções entre educação, formação e capacitação, bem como os meios para produzir um programa de capacitação.

O Capítulo III desta dissertação apresentará uma exposição e posterior reflexão sobre os programas de capacitação ou sensibilização, em cibersegurança ou em tecnologias de informação, desenvolvidos por congéneres do Centro Nacional de Cibersegurança, por organismos governamentais, bem como por organizações nacionais, da Europa e dos Estados Unidos da América, com real preocupação sobre esta temática e com evidências implementadas.

O capítulo IV será destinado às políticas públicas, desenvolvidas pelos Estados e União Europeia, que são catalisadoras do desenvolvimento das sociedades e da promoção da inovação tecnológica.

No capítulo V será focado o principal objeto desta dissertação, isto é, o desenvolvimento de um programa de ciber-higiene que contribuirá entre outros, para a consciencialização em cibersegurança dos cidadãos. Neste capítulo são ainda identificadas as principais etapas do programa, como sendo, o planeamento, o desenvolvimento do material de sensibilização e a implementação do programa. A escolha da metodologia de aprendizagem, bem como as ferramentas necessárias para transmitir os conteúdos de forma atrativa e dinâmica no processo de aprendizagem dos cidadãos é outros dos tópicos bordados neste capítulo. Por fim, abordamos as necessidades de competências de cibersegurança estratificadas por área funcional e dimensão da cibersegurança para sugerirmos um completo programa de capacitação para cidadãos.

O Capítulo VI concluirá esta dissertação e fornecerá uma sugestão de trabalho futuro, como forma de contributo para o desenvolvimento de competências em cibersegurança.

Não é objetivo deste trabalho apresentar o programa de capacitação de cidadãos em cibersegurança perfeito, até porque o mesmo não existe. Pretende-se, sim, apresentar um conjunto de recursos que possibilitem capacitar cidadãos na resposta aos desafios colocados pelas novas tecnologias e pelo ambiente digital e, simultaneamente tirar proveito dessa capacitação em segurança no uso dessas mesmas tecnologias no contexto organizacional.

1.2. O problema

No domínio da cibersegurança, os utilizadores são frequentemente designados como "o elo mais fraco" (K. & W., 2014, p. 361). O último relatório da IBM Security e Ponemon Institute (IBM Security & Ponemon Institute, 2017) estima que o custo dos incidentes referentes a quebras de segurança nas organizações, nos Estados Unidos da América (EUA), aumentou. Destes incidentes, 31% foram causados por negligência dos funcionários.

Os comportamentos de risco dos utilizadores são responsáveis por muitos ataques de cibersegurança e representam uma causa considerável no aumento dos ataques bem-sucedidos (Paganini, 2013). A este respeito, refere Paganini (2013) que "*novas oportunidades de negócios (on-line), plataformas móveis, armazenamento na nuvem e redes sociais são consideradas áreas privilegiadas de obtenção de sucesso sobre utilizadores não conscientes das possíveis ameaças de cibersegurança*" (Paganini, 2013).

Por outro lado, alguns tipos de comportamento de risco, também resultam em falhas de segurança que, não materializando ataques de cibersegurança de facto, resultam na criação de condições de vulnerabilidade que aumentam a exposição tecnológica a esses ataques. Exemplos desses comportamentos poderão ser não encerrar as sessões nas contas das aplicações, a partilha de credenciais de *login*, preencher formulários com informações pessoais sem saber se a origem é fidedigna (Paganini, 2013), visualizar emails de *phishing*[3], não reportar dispositivos roubados (Ranger,

[3] Como o nome em Inglês sugere, "*phishing*" significa "pescaria" e tem o objetivo "pescar" informações e dados pessoais importantes através de mensagens falsas.

2014), não julgar saber se poderá estar a ser vítima de engenharia social (definida como "*a arte de ganhar confiança ou aceitação para persuadir alguém a fornecer informações ou a realizar uma ação para beneficiar o atacante*" (Nakamura & Geus, 2007), utilizar *passwords* curtas ou pouco seguras (Athitakis, 2014), ou tomar más decisões na navegação na web, como clicar em janelas de publicidade (Blue, 2014), que podem ser usadas para disseminar *malware.*

Normalmente, os indivíduos que correm mais riscos são os menos informados, inocentes e pouco conscientes acerca dos princípios básicos da cibersegurança, o que consideramos relevante salientar, uma vez que "*muitos ataques externos - mais de 60% - são direcionados a funcionários via engenharia social*", que "*(…) exploram atividades através de e-mail e de redes sociais*" (Caldwell, 2013).

Os funcionários podem ser considerados como a primeira linha de defesa da organização contra o cibercrime e incidentes de Cibersegurança em geral, no entanto, também são o maior risco de segurança e a causa mais comum de violação de dados (Devaney, 2012). De facto, as atitudes passivas em relação à cibersegurança não são somente de indivíduos ou de funcionários com menos responsabilidades, mas também de administradores ou altos dirigentes com cargos de responsabilidade nas organizações. Muitos líderes consideram que a cibersegurança é um problema relacionado com as TIC, no entanto, são estes que têm a responsabilidade primária de criar uma cultura de segurança nas organizações que dirigem ou nas quais tem responsabilidades de gestão. Esta ideia é defendida por Posthumus e von Solms (Posthumus, 2004, p. 646), que afirmam que "*a governação da segurança da informação é uma questão complexa que exige o compromisso de todos da organização de forma a proteger os valiosos ativos de informações da empresa*".

É um facto que as organizações podem não conseguir eliminar completamente o risco de cibersegurança, no entanto se quem toma decisões estiver capacitado, consciente e formado nestes assuntos, mais facilmente consegue gerir o risco e tomar decisões acerca do investimento necessário ou a efetuar para mitigar o mesmo. Neste sentido, as organizações, além de infundirem a tecnologia nos seus modelos de negócio, também devem acompanhar a evolução digital, para que possam considerar a inclusão de medidas de cibersegurança um fator diferenciador de sucesso e de redução do risco.

Considerando que os incidentes de cibersegurança continuam a aumentar em frequência e sofisticação, as organizações devem tentar entender onde é que as violações de segurança dos dados tipicamente ocorrem. O relatório da IBM Security e Ponemon Institute (IBM Security & Ponemon Institute, 2017) apurou que o custo global médio de uma falha de segurança de dados é de US $3,62 milhões, o que representa um decréscimo de 10% em relação a 2016 (US $ 4 milhões). Neste estudo, globalmente, os custos diminuíram, no entanto em muitas regiões aumentaram. Este relatório revela

ainda que a resposta a incidentes, a criptografia e a educação (capacitação) foram os fatores com maior impacto na redução dos custos de violações de dados[4].

1.3. A missão do Centro Nacional de Cibersegurança

Na prossecução da missão atribuída ao Centro Nacional de Cibersegurança[5] (CNCS) – "*contribuir para que o País use 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 as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais*", o CNCS possui várias atribuições[6], sendo a mais relevante para o desenvolvimento desta dissertação, a atribuição de "*promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança*".

O programa de capacitação de cidadãos que nos propomos desenvolver neste trabalho vai totalmente ao encontro da consubstanciação de uma cultura nacional de cibersegurança.

[4] Ter uma equipa de resposta a incidentes (CSIRT) originou uma redução de US $ 19 no custo, por registo perdido ou roubado, seguido pelo uso extensivo de criptografia (redução de US $ 16 por registo) e formação adequada de funcionários (redução de US $ 12,5 por registo).

[5] Decreto-Lei n.º 69/2014

[6] a) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques; b) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança; c) Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais; d) Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais; e) Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança; f) Assegurar a produção de referenciais normativos em matéria de cibersegurança; g) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança; h) Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio; i) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros; j) Exercer as demais competências que lhe sejam atribuídas por lei.

1.4. O papel da Estratégia Nacional de Segurança do Ciberespaço

Na última década verificou-se uma maior preocupação por parte dos Estados relativamente à segurança no ciberespaço. Neste sentido, foram vários os países a desenvolver estratégias nacionais de segurança no ciberespaço (ou de Cibersegurança).

As várias estratégias desenvolvidas e analisadas assentam em pilares de certa forma semelhantes, apresentando contudo diferentes visões e orientações para assegurar os seus principais objetivos, que genericamente são a proteção da informação e das IC, a garantia de uma utilização segura do ciberespaço por parte cidadãos, e o incentivo para uma cooperação internacional capaz de aproveitar as infinitas potencialidades oferecidas pelo ciberespaço, de uma forma segura e responsável, sem colocar em perigo os interesses nacionais, nem os de outros sujeitos internacionais.

A consideração, pela Estratégia Nacional de Segurança do Ciberespaço (ENSC)[7], da cibersegurança como prioridade nacional assenta assim na consciencialização do Estado para os riscos que o desenvolvimento acelerado da sociedade de informação e dependência das TIC acarretam. Neste contexto, o Governo Português sentiu necessidade de garantir a proteção das IC e dos serviços de informação, bem como potenciar uma utilização livre, segura e eficiente do ciberespaço pelos cidadãos, empresas e organismos públicos.

A ENSC (a que nos referiremos em diante como Estratégia) conjuga os princípios estruturais do Estado português, com as linhas gerais da União Europeia para a Cibersegurança, em harmonia com a proteção do indivíduo consagrada na convenção Europeia dos Direitos do Homem e da Carta dos Direitos Fundamentais da União Europeia. As necessidades associadas a cada um dos objetivos estratégicos[8] e as suas implicações levaram à definição de uma orientação estratégica que foi traduzida em seis eixos de intervenção[9].

[7]Aprovada em 12 de junho de 2015 através da Resolução do Conselho de Ministros n. º36/2015

[8] a) promover uma utilização consciente, livre, segura e eficiente do ciberespaço; b) proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; c) fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; d) afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

[9] Eixo 1 — Estrutura de segurança do ciberespaço; Eixo 2 — Combate ao cibercrime; Eixo 3 — Proteção do ciberespaço e das infraestruturas; Eixo 4 — Educação, sensibilização e prevenção; Eixo 5 — Investigação e desenvolvimento; Eixo 6 — Cooperação.

A Estratégia assenta ainda em cinco pilares estruturantes, a saber, a subsidiariedade[10], a complementaridade[11], a cooperação[12], a proporcionalidade[13] e a sensibilização[14].

Dos seis eixos de intervenção, destaca-se para o âmbito do presente trabalho o eixo quatro da Estratégia, que refere que "*o sucesso da segurança do ciberespaço passa pela promoção de uma cultura de segurança que proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização dos sistemas de informação, reduzindo a exposição aos riscos do ciberespaço*" e, refere ainda, que deve ser adotada, entre outras, a seguinte medida: "*1) Promover campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas*". Neste contexto, os instrumentos e as medidas de sensibilização na temática do uso seguro e responsável das TIC, devem ser criados para uso da sociedade civil.

Como plano de ação para a operacionalização deste eixo— educação, sensibilização e prevenção, e do quinto pilar estruturante – a sensibilização, consideramos que se torna premente o desenvolvimento de um programa genérico de capacitação para os cidadãos.

1.5. Iniciativa Portugal INCoDe.2030

A Iniciativa Portugal INCoDe.2030[15] tem como missão apoiar a criação de uma sociedade mais resiliente, estimulando nos cidadãos o desenvolvimento de competências digitais, que se encontram em persistente transformação e desenvolvimento.

---

[10] Subsidiariedade – a segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço. O Estado afirma o seu forte compromisso com a proteção do ciberespaço. No entanto, grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida por operadores privados, a quem cabe a responsabilidade primária pela sua proteção. Esta responsabilidade inicia-se no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais.

[11] Complementaridade – a segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais. Uma abordagem alargada e integradora da segurança do ciberespaço reúne diferentes atores com diferentes responsabilidades e capacidades, para benefício de todos.

[12] Cooperação - num mundo altamente interligado e interdependente, a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais, alicerçada no desenvolvimento de confiança mútua

[13] Proporcionalidade - os riscos inerentes ao ciberespaço devem ser avaliados e geridos de forma adequada, assegurando -se a proporcionalidade dos meios e medidas para o seu exercício.

[14] Sensibilização - a garantia da segurança das infraestruturas tecnológicas, das redes e dos sistemas de informação depende da capacidade de os utilizadores finais saberem tomar medidas que previnam os riscos a que se encontram expostos. A sensibilização constitui um eixo essencial à preservação da segurança no ciberespaço

[15] http://www.incode2030.gov.pt/

Esta iniciativa está integrada num programa de contexto internacional, sendo objetivo nacional que Portugal garanta um lugar destacado em competências digitais no período 2017-2030, respondendo para este efeito a três grandes desafios[16], sendo de destacar, para o exercício da exequibilidade deste trabalho, o primeiro deles – "Garantir a literacia e a inclusão digitais para o exercício pleno da cidadania". Um abrangente conjunto de medidas, movimentadas por organismos governamentais e articuladas com as iniciativas da sociedade civil, pretendem assim enfrentar os desafios e metas propostos, organizando-se segundo cinco eixos principais de ação: inclusão, educação, qualificação, especialização e investigação.

Consciente de que o mundo contemporâneo atravessa uma progressiva digitalização presente em todos os domínios do saber, neste sentido, torna-se imprescindível munir o cidadão de capacidades e meios de acesso e utilização das tecnologias digitais. O programa de capacitação de cidadãos em cibersegurança que nos propomos desenvolver neste trabalho, encontra-se alinhado com o eixo 1 – Assegurar a generalização do acesso às tecnologias digitais a toda a população, para obtenção de informação, comunicação e interação e com o eixo 3- Capacitar profissionalmente a população ativa dotando-a dos conhecimentos necessários à integração num mercado de trabalho que depende fortemente de competências digitais, do INCoDe2030, estimulando-nos para a implementação do mesmo, alinhado com a temática da utilização segura dessas tecnologias.

[16] 1. Garantir a literacia e a inclusão digitais para o exercício pleno da cidadania, 2. Estimular a empregabilidade e especialização em tecnologias e aplicações digitais para a qualificação do emprego e uma economia de maior valor acrescentado, 3. Produzir novos conhecimentos nas áreas digitais em cooperação internacional.

2. Educação, formação e capacitação

Nos últimos anos cresceu a consciência, por parte dos decisores das organizações, da necessidade de gerir os riscos de cibersegurança. Esta tomada de consciência deve-se ao facto de praticamente todas as organizações terem evoluído para um modelo de negócio assente no digital. Conjuntamente com esta evolução surgiu o aumento da necessidade de as organizações terem os seus próprios especialistas em cibersegurança, bem como a expansão dos serviços de cibersegurança, prestados por terceiros

Em 2014 foi publicado um relatório do Governo do Reino Unido (HM Government, 2014) onde foram apresentados resultados relativamente à necessidade de competências em cibersegurança por parte das empresas. Este relatório enfatizou a necessidade de profissionais com vastas competências técnicas, mas também a necessidade de novos trabalhadores com competências empresariais mais fortes e maior experiência de trabalho. Também identificou a importância de aumentar, nos profissionais que criam, compram e usam tecnologia, as competências em cibersegurança com o objetivo de reduzir as vulnerabilidades do negócio relativamente aos incidentes de cibersegurança e entre os decisores das organizações com responsabilidade na gestão do risco do negócio.

Naturalmente, uma carreira em cibersegurança requer competências relevantes e, em certos casos, muito específicas. Pelo facto de, à data atual, não existir um quadro identificativo das competências ditas relevantes, pode-se encontrar no mercado uma variedade imensa de cursos de formação e de ensino, tipicamente conotados como cursos de requalificação ou reconversão, sendo que somente alguns conduzem a qualificações formais. É efetivamente um verdadeiro desafio para quem procura qualificar-se, preparar-se para entrar ou desenvolver uma carreira em cibersegurança escolher o curso/formação.

Necessidades de competências

O ponto de partido deverá ser a identificação das necessidades de competências que contribuem para a melhoria das qualificações em cibersegurança e, só posteriormente, se poderá encontrar a oferta formativa de cursos de requalificação ou reconversão, alinhados com as necessidades previamente identificadas.

Neste âmbito, existem ainda algumas questões que devem ser consideradas antes da procura dos cursos de formação ou educação:

- Necessidade de qualificação – Os cursos de requalificação ou reconversão oferecem qualificações, que podem ser graus académicos ou certificações profissionais, mas muitas vezes a qualificação formal não é solicitada, pelo que a aquisição de conhecimento, por si só, é suficiente;
- Recursos e compromissos – Identificação dos recursos necessários para integrar um curso de requalificação ou reconversão, como por exemplo o custo financeiro ou o tempo de duração curso;

- Formato do curso - cursos presenciais que se desenrolam num longo período de tempo, obrigando os trabalhadores a estar ausentes ou menos presentes na sua organização por um longo período, outros exigem uma curta dedicação em termos de tempo (algumas vezes, apenas um dia), e outros ainda podem ocorrer remotamente (*on-line*);
- Prés requisitos em termos de conhecimentos - Alguns cursos iniciam-se com módulos de alinhamento de conhecimentos, enquanto outros têm como pré-requisito de entrada um determinado nível de conhecimentos;
- Direcionado à função - Muitos cursos de requalificação ou reconversão são direcionados a uma função específica, por exemplo à função de "Testes de penetração";
- Conhecer ou fazer – Alguns cursos de requalificação ou reconversão focam-se apenas no "conhecer", enquanto outros se concentram em "saber fazer", no entanto a maioria deles oferece uma combinação de ambos;
- Tecnologia predominante - Alguns cursos direcionam a abordagem dos seus conteúdos aplicados a uma tecnologia específica ou são muitas vezes tendenciosos relativamente a determinada tecnologia.

Em Portugal, ainda não existe um quadro com a identificação das competências relevantes para uma carreira em cibersegurança, no entanto, após pesquisa efetuada, identificamos na Europa (mais especificamente no Reino Unido), o Institute of Information Security Professionals **(**IISP)[17]que desenvolveu o *IISP Information Security Skills Framework* (The Institute of Information Security Professionals, 2017) .

O IISP é uma organização não governamental sem fins lucrativos e lançou a versão 2.1 do *Skills Framework* em *2017*. Este quadro foi desenvolvido pela primeira vez em 2006 (versão1.0), revisto em 2010 (versão 2.0) e contou com a colaboração de especialistas académicos e de segurança de renome mundial, com origem na indústria, no Governo e nas universidades. Atualmente, o *IISP Skills Framework* é usado pelo Governo do Reino Unido para sustentar o seu programa de certificação profissional e por organizações privadas para desenvolver e avaliar as capacidades de cibersegurança dos seus trabalhadores. Também é usado como inspiração no desenvolvimento de cursos de formação e cursos universitários de cibersegurança do Reino Unido.

Este quadro de referência contém a identificação das competências que os profissionais de cibersegurança devem ter para o desempenho das suas funções. O quadro foi desenvolvido, como referido anteriormente, com a colaboração de profissionais do sector público e privado, bem como da academia. Da análise que efetuamos, este quadro de referência foi identificado como uma estrutura simples e clara de avaliação comparativa de cibersegurança.

O *IISP Skills Framework* inicialmente era baseado nas seguintes áreas de competência, sendo que nem todas as funções necessitam de experiência em todas as categorias: gestão da segurança da informação; gestão do risco; implementação de sistemas seguros; metodologias de garantia da

[17] https://www.iisp.org

Informação e de testes; gestão da segurança operacional; gestão de incidentes; auditoria, garantia e revisão; gestão de continuidade de negócio e pesquisa de sistemas de Informação.

Posteriormente, e na sua versão 2.1 em 2017, o quadro evoluiu para que refletisse a evolução nas ameaças nas novas tecnologias e nas mudanças significativas nos perfis e desafios de competências em cibersegurança. O novo quadro inclui novas categorias, nomeadamente: avaliação de ameaças; modelação de ameaças; ciber resiliência; testes de penetração; deteção e gestão de análise de intrusão; investigação e resposta a incidentes. O novo quadro ampliou ainda as competências da função de técnico de arquitetura de segurança e redefiniu as competências do perfil de auditoria, conformidade e testes. Competências como a gestão, a liderança e a influência, competências organizacionais e de comunicação e partilha de conhecimento tiveram uma ênfase especial nesta última versão do quadro.

O Reino Unido tem também um "Programa Nacional de Cibersegurança", que tem como objetivo implementar a Estratégia Nacional de Cibersegurança no Reino Unido (HM Government, 2016). Este programa tem ainda por missão a partilha de conhecimentos, capacidades e competências em cibersegurança. Sendo desenvolvido pelo CESG[18], o Programa de Certificação da Formação da CESG (GCHQ Certified Training)[19] tem como objetivo garantir um nível elevado na qualidade dos cursos de requalificação em cibersegurança, através da certificação do *IISP Skills Framework*.

2.1. Educação e formação

Muito já foi escrito e dissertado (Masadeh, 2012) sobre as principais diferenças entre "educação" e "formação" e a maioria dos estudos sobre este tema também tem aplicabilidade na cibersegurança, para além de em outras disciplinas.

Simplificando as várias definições pesquisadas, a educação foca-se principalmente na aquisição de conhecimentos e na compreensão, através das quais as competências são desenvolvidas. Por outro lado, a formação foca-se na transferência específica das mesmas competências, com o objetivo de abordar lacunas em competências ou em conhecimentos já aprendidos.

No entanto, na carreira de cibersegurança, como em outras, existem situações e argumentos para pontualmente poder haver um investimento tanto em educação como em formação. Um exemplo do que acabamos de referir poderá ser uma carreira em Gestão de Incidentes de cibersegurança (comummente designada de *Incident Handler*), onde para além da constante necessidade de adquirir e desenvolver novas competências que acompanhem a rápida evolução da tecnologia associada às atividades de resposta (e também de ataque), existe a necessidade de, face a essa evolução, manter um elevado nível de conhecimento e competências através da formação contínua, que nesta carreira em particular decorre com especial intensidade por iniciativa do próprio formando.

Fundamentalmente, podemos afirmar que um dos principais papéis da educação é preparar alguém para o futuro, enquanto a formação tem muito mais a ver com o "aqui e agora". Na cibersegurança, como noutras áreas, a educação e a formação complementam-se muito

[18] https://www.gov.uk/government/organisations/cesg
[19] https://www.ncsc.gov.uk/scheme/gchq-certified-training

confortavelmente, uma vez que a progressão numa função de cibersegurança deve ser participada por um envolvimento prudente em ambas as atividades.

2.2. Formação e capacitação

Após estar clarificada a distinção entre educação e formação, importa também efetuar a distinção entre formação e capacitação. Tal como referido no ponto anterior, formação tem como objetivo ensinar competências que permitam a um indivíduo desempenhar uma função específica, enquanto a capacitação tenta focar a atenção de um indivíduo num problema ou num conjunto de questões, nas quais é premente a sua perceção e a adequação do seu comportamento.

Neste sentido, um programa de capacitação de indivíduos em cibersegurança é apenas um dos elementos críticos de umas necessárias abrangentes medidas de educação e sensibilização em cibersegurança. Por outro lado, é também o principal canal para facultar aos funcionários as ferramentas e a informação necessária para proteger os recursos vitais da informação de uma organização.

Estes programas de capacitação permitem que todos os funcionários de uma organização entendam as suas responsabilidades e usem e protejam adequadamente as informações e os recursos que lhes são confiados. Acreditamos convictamente que as organizações que facultam periodicamente formação e treino aos seus funcionários, em políticas e responsabilidades de cibersegurança, terão uma maior taxa de sucesso na segurança da sua informação e das suas redes.

Oos indivíduos são indiscutivelmente o elemento mais fraco da fórmula de cibersegurança, que é usada para proteger sistemas e redes. Não a tecnologia, mas sim o indivíduo, é o fator crítico, muitas vezes ignorado nesta equação da cibersegurança. Programas de capacitação em cibersegurança, robustos e transversais a todas as organizações e ao cidadão comum, são assim essenciais para abordar esta crescente preocupação.

Uma organização que investe na formação em cibersegurança dos seus funcionários é uma organização que fomenta o desenvolvimento das competências, fornecendo relevantes conhecimentos e proficiências de segurança da informação.

2.2.1. Formação em Cibersegurança

A formação é tipicamente ministrada em módulos e/ou cursos adaptados às necessidades específicas de um determinado grupo de indivíduos, que foram previamente identificados com funções e responsabilidades comuns ou relacionadas entre si, na cibersegurança.

Aquando da criação de módulos e cursos de formação, devem ser considerados os seguintes elementos críticos: a obsolescência dos conteúdos e a consequente necessidade de atualização dos mesmos. Neste sentido, deve estar prevista uma revisão e consecutiva atualização de conteúdos de forma periódica.

2.2.2.Capacitação

A capacitação em cibersegurança deve combinar atividades de promoção de segurança, estabelecer responsabilidades e comunicar aos funcionários as últimas notícias e novidades de cibersegurança. O objetivo de um programa de capacitação é tentar que o indivíduo se foque num problema ou num conjunto de questões. Estes programas devem disseminar continuamente, e através de vários formatos, a mensagem de cibersegurança pelos indivíduos utilizando uma multiplicidade de ferramentas, meios de comunicação e divulgação, e desenvolvimento de métricas:

Ferramentas

O objetivo primordial das ferramentas de capacitação centra-se na promoção da cibersegurança e na informação aos utilizadores sobre as ameaças e vulnerabilidades a que está sujeita a organização e o seu ambiente de trabalho. Esclarecendo sempre o "que não é permitido fazer", explicando as regras de comportamento aquando da utilização dos sistemas de informação de uma organização e estabelecendo um nível de expectativa sobre o uso aceitável do mesmo. Um programa de capacitação não só deve comunicar políticas e procedimentos de cibersegurança que devem ser seguidos, mas também facultar informação sobre as sanções pela não conformidade a essas políticas e procedimentos.

Exemplos de tipos de ferramentas, poderão ser eventos de sensibilização em organizações, concursos de cartazes de cibersegurança, exercícios de cibersegurança, matérias promocionais com conteúdos de boas práticas e regras de comportamento, pequenas reuniões com equipas restritas de colaboradores, poster com boas práticas, cursos genéricos de cibersegurança, cursos de cibersegurança específicos para determinada carreira profissional, cursos de E-Learning, conferências, entre outras.

Comunicação

O esforço de um programa de capacitação centra-se fundamentalmente na comunicação do mesmo aos utilizadores, aos decisores, aos dirigentes e aos responsáveis pelo sistema informático, entre outros. Para garantir o sucesso do programa torna-se necessário a existência de um plano de comunicação que identifique claramente as partes interessadas, os tipos de informação a divulgar, os canais de divulgação e a frequência com que irão ocorrer. Também a avaliação e o plano estratégico de implementação do programa são atividades que suportam a comunicação.

Divulgação

Para garantir o impulso e sucesso das melhores práticas de cibersegurança nas organizações é necessário que o âmbito de aplicabilidade dessas práticas seja suficientemente grande, sendo que neste sentido podem ser considerados programas intra e interorganizações.

Pode ser desenvolvido um portal Web que aloje num ponto único tudo o que se refere à capacitação em cibersegurança e onde políticas, perguntas frequentes (FAQs), *newsletters* de cibersegurança, links para recursos e outras informações úteis poderão ser facilmente acedidos por todos os funcionários neste ponto único. Este portal deve promover uma mensagem consistente e padrão. O facto de o portal poder ser utilizado em ambiente interorganizacional é particularmente

relevante, uma vez que estimula a partilha de informação e conhecimento entre organizações e alavanca os recursos e a diversidade de experiências de capacitação.

Certificação

Respondendo à crescente necessidade de técnicos de cibersegurança nas organizações, tanto no setor público como no setor privado, tem-se verificado a criação e oferta de uma variedade considerável de cursos profissionais, educacionais ou de especialização, entre outros. Como forma de validação de conhecimentos, estes cursos têm mecanismos de avaliação que poderão resultar numa certificação de conhecimentos e habilitação de determinado nível de competência.

3. Principais programas de capacitação em cibersegurança

3.1. Na Europa

Os incidentes de cibersegurança ocorrem cada vez com maior frequência e com maior impacto. Os órgãos de comunicação social fazem das vulnerabilidades de segurança, e das repercussões dos mesmos, notícia de destaque, sendo importante realçar que as repercussões destes acontecimentos podem ter impacto significativo em Estados, organizações e cidadãos. Tipicamente há a perceção de que apenas grandes organizações estão em risco e são visadas pelos autores destes ataques, no entanto, são milhares (e significativos) os incidentes e ataques contra as Pequenas e Médias Empresas (PME's), não conhecidos, reportados ou mesmo divulgados.

Notavelmente, os ataques bem sucedidos alavancam problemas de segurança conhecidos de todos nós. Cerca de 80% dos ataques ocorridos, tiveram como fundamento a falta de boas práticas de cibersegurança nas organizações [20].

Não é com certeza de menosprezar o desenvolvimento de um programa de capacitação de cidadãos. Com a aplicação destas medidas, serão minimizados os riscos de um indivíduo se tornar vítima de um ataque de cibersegurança ou de ser veículo de propagação do impacto do ataque por outras organizações. Neste contexto, o programa de capacitação deve ser integrado adequadamente numa organização, como uma simples rotina periódica em que os bons comportamentos e os check-ups ocasionais sirvam para garantir a saúde da cibersegurança das organizações.

Em 2013, o ataque à cadeia de lojas norte americana Target foi um infeliz exemplo de um sistema de pagamento vulnerável a um incidente de cibersegurança, que expôs dados bancários de cerca de 40 milhões de clientes. "O acesso não autorizado" ao sistema afetou os clientes que pagaram com cartões de crédito ou de débito.

Embora, no caso da Target o investimento em segurança e em estratégias para que situações semelhantes não se repetiam não seja um obstáculo, já no caso da maioria das PME a luta para ter recursos, acesso ou conhecimento necessários para fazer face à implementação de medidas de cibersegurança pode ser uma dificuldade. Torna-se então imperativo uma maior ênfase na ciber-higiene, de modo a ajudar as empresas a proteger toda a comunidade, bem como a si mesmos.

Atualmente, na Europa, não existe uma abordagem única, ou comummente ajustada, sobre capacitação de cidadãos em cibersegurança, tendo cada um dos Estados os seus próprios programas e orientação. No entanto, e predominantemente, esses programas encontram-se alinhados ou mesmo orientados pelas Estratégias Nacionais de Cibersegurança publicadas[21] por cada País.

[20] Relatório do Governo do Reino Unido - CESG (the Information Security Arm of GCHQ) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

[21] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Os programas da Bélgica, França e Reino Unido encontram-se num estado de suficiente maturidade para que possam servir de inspiração e adaptação para quem os queira seguir. Do mesmo modo, o Instituto Nacional de Ciência e Tecnologia dos Estados Unidos (NIST) também produziu e disponibiliza um guia para a capacitação em cibersegurança.

Bélgica - Parceria público-privada- ICC Bélgica, FEB, EY, Microsoft, L-SEC, B-CCENTRE e ISACA Bélgica

Desta parceria público-privada resultou um guia de cibersegurança[22], agnóstico da indústria e da tecnologia, com informação de alto nível e organizado para dar conselhos sobre boas práticas.

O documento está dividido em duas partes principais: os 10 Princípios de Segurança, que devem ser adotados por todas as empresas e as 10 Ações de Segurança "must do", cujo objetivo é transformarem princípios em orientações. Existe também um questionário de autoavaliação que possibilita que os indivíduos explorem cada área de ação ou princípio e obtenham uma visão do que devem atender na sua organização. Posteriormente existem 16 áreas com questões (5 perguntas por área), em que os utilizadores podem responder de 3 formas distintas: "fazemos isto de forma adequada", "podemos melhorar", e "não estamos a fazer". As questões do questionário de autoavaliação estão vinculadas aos princípios relevantes e às ações de atuação obrigatória.

Este programa não permite uma certificação formal, no entanto, é possível que as questões do questionário de autoavaliação possam ser usadas como atestado durante uma auditoria de cibersegurança.

França - Agência Francesa de Segurança dos Sistemas de Informação - ANSSI[23]

40 Medidas Essenciais para uma Rede Saudável[24]

Estas 40 Medidas Essenciais para uma Rede Saudável materializam-se num guia que abrange 13 áreas de controlo e pretende orientar os utilizadores em profundidade. A base mínima para a cibersegurança, preconizada pela ANSSI, traduz-se nas medidas essenciais. Este guia não exige implementações específicas nem opções de tecnologia. A primeira versão foi produzida em 2013 e no presente ano sairá uma versão atualizada das 40 medidas.

As áreas de controlo (Anexo B) são orientadas para o dia-a-dia do contexto empresarial (existe em separado a área de sistemas SCADA/ICS). Atualmente não existe nenhuma forma que permita às organizações verificarem o cumprimento das 40 medidas essenciais.

Guia de Boas Práticas Informáticas[25], produzido pela CGPME/ANSSI.

[22] https://www.b-ccentre.be/wp-content/uploads/2013/11/BCSG.pdf

[23] https://www.ssi.gouv.fr/en/

[24] https://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_v1-2-1_en.pdf

[25] https://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

As 40 medidas revelaram-se complexas em tamanho e perceção, pelo que foi produzida uma versão reduzida de 12 regras destinadas às PME. A limitação deste documento está no idioma, pois apenas está disponível em Francês, o que limita a aplicabilidade em toda a Europa.

Este guia de boas práticas é acessível a profissionais de TI, a especialistas e a não especialistas, sendo este um reflexo da sua adaptabilidade às PME. À imagem das 40 medidas essenciais, também aqui não existe um processo de acreditação, verificação ou avaliação de conformidade das 12 regras à organização.

Reino Unido – *Cyber Essentials* - UK Government [26]

Como forma de combater os ataques de cibersegurança detetados pelas agências nacionais de segurança, foi desenvolvida uma orientação - *Cyber Essentials*, para identificar os controlos técnicos e básicos necessários. Esta iniciativa foi desenvolvida pelo Governo do Reino Unido conjuntamente com o consórcio de segurança da informação para as PME (IASME) e com o Fórum de Segurança da Informação (ISF).

Neste guia existem apenas 5 áreas de controlos e o destaque é dado à área do controlo de infraestrutura física. Surpreendentemente, os serviços na nuvem e os controlos de segurança da camada de aplicação não são refletidos. O guia fornece um modelo de "certificação", ao qual as empresas que aderem ao programa podem ser verificadas e demonstrar conformidade com clientes e parceiros de negócios. A certificação é atribuída em dois níveis: versão de autoteste e versão independente verificada tecnicamente (*Cyber Essentials Plus*). Aquando da obtenção da certificação, as empresas podem colocar os logotipos do *Cyber Essentials* na sua documentação e no seu *site*. Em outubro de 2016 existiam aproximadamente 4.000 empresas certificadas.

3.2. Nos Estados Unidos da América

EUA - Instituto Nacional de Ciência e Tecnologia (NIST)[27]

O Instituto Nacional de Ciência e Tecnologia (NIST) dos EUA, em novembro de 2016, publicou a revisão 1 da NISTIR 7621 - "*Small Business Information Security: The Fundamentals"*, cujo objetivo é ajudar as pequenas empresas a aplicar controlos de segurança básicos à informação, sistemas e redes.

Tipicamente, os proprietários das PME pensam que as suas organizações têm uma dimensão reduzida para serem vítimas de incidentes de cibersegurança, mas Celia Paulsen e Patricia Tothsabe (Paulsen & Tothsabel, 2016) consideram o contrário. As autoras lideram esforços de divulgação da cibersegurança nas PME e entendem os desafios que essas empresas enfrentam na proteção dos seus dados e sistemas. "*Todas as empresas, sejam de que dimensões forem, enfrentam riscos potenciais quando estão on-line, logo, necessitam de ter em linha de conta a segurança da informação*".

[26] https://www.ssi.gouv.fr/en/

[27] https://www.nist.gov/

NIST's *Small Business Information Security: The Fundamentals* é um guia dirigido aos proprietários das PME, sem experiência em cibersegurança, e explica os passos básicos a adotar para proteger melhor os sistemas de informação. Explica por exemplo, como criar políticas de acesso aos dados e às informações, como dar formação aos funcionários sobre segurança da informação, como criar políticas e procedimentos para a segurança da informação; como cifrar dados; como instalar *patch,* atualizações, sistemas operativos e aplicações, entre outros. O guia sugere também alguns conselhos sobre sistemas básicos que qualquer empresa deve ter, exemplificando: sugere a utilização de um sistema de UPS, que permite continuar a trabalhar mesmo quando ocorre um corte de energia, permitindo assim salvar a informação; sugere a gestão do risco, de forma a determinar o valor dos seus ativos de informações e a priorizar os controlos de segurança, entre outros. Segundo dados da National Cyber Security Alliance[28], 60% das PME encerram a sua atividade, seis meses após um efetivo ataque de cibersegurança.

Este guia, bem como o guia belga e o francês, não permitem certificar a sua conformidade ou usar a certificação para atestar o nível de segurança junto do fornecedor.

Foi introduzida uma legislação nos EUA, em outubro de 2016, para fazer face aos ataques de cibersegurança contra redes informáticas - The Promoting Good Cyber Hygiene Act[29]. Esta legislação é fruto de uma ordem executiva[30], de 2013, do Presidente Barack Obama. O presidente do EUA instruiu o NIST, juntamente com a Federal Trade Commission e o Department of Homeland Security, para produzir boas práticas para segurança das redes e da informação.

Em agosto de 2017, a National Initiative for Cybersecurity Education (NICE), liderada pelo NIST do Departamento de Comércio dos EUA, estabeleceu uma parceria entre Governo, academia e setor privado e trabalharam no sentido da dinamização e da promoção de uma rede robusta e de um ecossistema de educação, formação e desenvolvimento em cibersegurança, destinado aos trabalhadores. Nesta iniciativa conjunta entre parceiros governamentais, académicos e indústria, a NICE teve como missão o desenvolvimento de programas (bem-sucedidos), facilitadores da mudança e da inovação, cujo objetivo final era aumentar o número de profissionais qualificados em cibersegurança e assim apoiar na manutenção de um Estado mais seguro.

A NICE mantém-se focada na promoção de iniciativas nacionais, que aumentem o número de trabalhadores com conhecimentos, competências e capacidades na execução das tarefas necessárias em cibersegurança.

A NIST Special Publication 800-181[31] é um referencial de apoio às organizações, que utiliza um vocabulário comum e consistente para descrever o trabalho em cibersegurança segmentado em categorias, especialidade e função. Esta publicação descreve os conhecimentos, competências,

[28] https://staysafeonline.org/stay-safe-online/resources/

[29] https://www.congress.gov/bill/114th-congress/house-bill/3664

[30] http://eshoo.house.gov/issues/economy/eshoo-bill-vaccinates-against-majority-of-hacks-with-cyber-hygiene-network-security-management/

[31] https://doi.org/10.6028/NIST.SP.800-181

capacidades e tarefas de cibersegurança para cada função. O *NICE Framework*[32] é um documento orientador e de suporte à comunicação organizacional e sectorial, relativamente à educação, formação e desenvolvimento da carreira dos trabalhadores em cibersegurança.

Figura 1 – Construção de uma carreira de cibersegurança

O utilizador do *NICE Framework* deve adaptar esta publicação aos padrões, regulamentos, necessidades e missão da organização onde está inserido. Desta forma, esta é apenas um ponto de partida relativamente às orientações e diretrizes de um programa de gestão de carreira, educação, formação e credenciação na área de cibersegurança.

3.3. Em Portugal

Centro Internet Segura - Portugal[33]

Em 1999 a Comissão Europeia lançou o programa Safer Internet e posteriormente em 2005 lançou o programa Safer Internet Plus, com o objetivo de dinamizar projetos nos Estados Membros de promoção da utilização segura da Internet. Em Portugal, no âmbito deste programa, a Direção Geral de Inovação e Desenvolvimento Curricular, através da Equipa de Missão Computadores, Redes e Internet (DGIDC-CRIE) do Ministério da Educação, desenvolveu, em 2004, o projeto SeguraNet, cujo objetivo era a promoção de uma utilização esclarecida, crítica e segura da Internet junto dos estudantes do ensino básico e secundário. No programa do Governo de 2005, uma das orientações estratégicas

[32] https://doi.org/10.6028/NIST.SP.800-181, pag. 7

[33] Entrevista à Dra. Sofia Rasgado (Coordenadora do Centro Internet Segura, Departamento da Sociedade da Informação) no dia 10 de outubro de 2017 e à Dra. Lígia Azevedo (Equipa SeguraNet da Direção Geral da Educação) no dia 12 de outubro de 2017

do programa LigarPortugal, era "*Assegurar a Segurança e a Privacidade no Uso da Internet*", mais especificamente "*garantir que todos, e em particular as famílias, dispõem de instrumentos para proteção de riscos que possam ocorrer no uso da Internet e têm informação sobre como os utilizar*". O projeto Internet Segura contribuiu para a concretização desta orientação estratégica.

Desde 2004 que o SeguraNet é o centro de sensibilização para as questões da cidadania digital nas comunidades educativas e faz parte da rede de Centros Internet Segura, rede INSAFE, constituída por 33 países.

A missão da rede de cooperação INSAFE tem como objetivo capacitar os cidadãos a usarem a internet, os telemóveis, os *tablets*, bem como outras tecnologias *online*, de forma positiva, segura e eficaz. A INSAFE exige uma responsabilidade partilhada na proteção dos direitos e necessidades dos cidadãos, em particular das crianças e jovens, por parte do Governo, educadores, pais, comunicação social e indústria, entre outros atores relevantes, dando especial relevo à eliminação da pornografia infantil. Os parceiros da INSAFE trabalham em estreita colaboração, de forma a partilharem as melhores práticas, informações e recursos, interagindo com a indústria, escolas e famílias tendo como objetivo a capacitação dos cidadãos, colmatando a divisão digital entre o lar e a escola e entre as gerações.

A rede INSAFE tem desenvolvido inúmeras iniciativas e ferramentas de conscientização para capacitar crianças, jovens e cidadãos em geral, com o objetivo os manter seguros na Internet, Salienta-se a organização, dentro e fora da Europa, do Dia da Internet mais segura, que ocorre no segundo dia da segunda semana de fevereiro, desde 2004.

Em Portugal, o Centro de Internet Segura (PT CIS) - é uma parceria de cinco organizações (Direção-Geral da Educação, Fundação para a Ciência e Tecnologia, Instituto Português do Desporto e Juventude, Microsoft Portugal e a Fundação Portugal Telecom) cujo principal trabalho e experiência são bastante relevantes para tornar a Internet mais segura. O PT CIS é co-financiado pela Comissão Europeia, através do Connecting Europe Facility (CEF) e parte da rede INSAFE que abrange mais trinta centros europeus desse tipo, com foco em três áreas principais: conscientização, linha de atendimento e uma linha direta.

A sua linha de atuação passa pela formação de professores e de colaboradores de outras entidades, pela dinamização de sessões de sensibilização nas Escolas, pela disponibilização informação/recursos em múltiplos formatos para cada um dos seus públicos e pela dinamização de diversas iniciativas dirigidas à comunidade educativa.

O Projeto do Centro de Internet Segura tem os seguintes objetivos estratégicos: o combate a conteúdos ilegais; a minimização dos efeitos de conteúdos ilegais e lesivos nos cidadãos; a promoção de uma utilização segura da Internet; e a consciencialização da sociedade para os riscos associados à utilização da Internet. Estes objetivos estratégicos têm sido cumpridos através de, entre outros, da criação de um serviço *online* para denúncia de conteúdos ilegais; da disponibilização de informação sobre os perigos associados à utilização da Internet, da disponibilização de conteúdos informativos, formativos e interativos relevantes para a utilização segura da Internet e da promoção do envolvimento do sector privado em ações que promovam a utilização da Internet em Segurança.

No seu último relatório publicado[34], de junho de 2016, destaca-se entre outras, a continuação da promoção do concurso Desafios SeguraNet que envolve estudantes, professores e pais, abrangendo anualmente cerca de 50 000 participantes; a continuação da realização de cursos de capacitação para professores e profissionais que trabalham com crianças vulneráveis; contribuir para a nova integração curricular sobre os problemas de segurança digital e a continuação da formação de professores de 1º ciclo que apoiem a iniciativa: Introdução ao Código no 1º ciclo.

Pelo cumprimento da missão da PT CIS, muitos esforços têm sido desenvolvidos na produção de ferramentas, recursos e campanhas criativas, educacionais e adequadas para envolver e motivar crianças, jovens, professores, assistentes sociais, adultos e idosos a considerar sua própria segurança *online*. A necessidade de construir e fortalecer uma rede com todas as partes interessadas e envolvidas na cibersegurança, nomeadamente instituições públicas e privadas e organizações do sector terciário uniram-se num espírito cooperativo para reforçar a mensagem positiva sobre o uso das tecnologias digitais.

Neste sentido, dois órgãos de consultoria interagem com o PT CIS para melhor desenhar e preparar os recursos e campanhas:

- O Lideres Digitais, para as escolas portuguesas, que visam melhorar o conhecimento e as competências de um uso mais seguro da Internet e dos dispositivos móveis, dentro das comunidades educativas, através da aprendizagem não formal de estudantes selecionados (dos 9 aos 18 anos), durante o ano letivo. Esta divulgação de competências é conseguida de fora exímia através do desenvolvimento de sessões de conscientização, não formais, promovidas pelos estudantes de líderes digitais nas suas comunidades educativas, utilizando as competências adquiridas e os materiais educacionais propostos. Estes estudantes - Líderes Digitais, também atuam como conselheiros privilegiados tanto da SeguraNet como do Centro Internet Segura. Em cada comunidade educacional existe, pelo menos, um professor responsável pelos alunos e atividades. Na 2.ª edição (2016/17) participaram cerca de 40 comunidades educativas com 162 Líderes Digitais e na 3ªedição, a que se encontra em curso (2017/18) encontram-se a participar cerca de 600 Líderes Digitais.
- Conselho Consultivo - Este órgão é constituído por entidades e personalidades com conhecimentos reconhecidos e responsabilidades no desenvolvimento da Sociedade da Informação em Portugal, bem como direitos e proteção dos jovens e crianças. Atualmente colaboram 23 instituições neste conselho.

Algumas das ações que contribuíram para o aumento da sensibilização e das atividades educativas:

- Dia da Internet Mais Segura: em fevereiro de cada ano, a rede Insafe, promove uma campanha que visa a utilização crítica e responsável da tecnologia e dos dispositivos móveis, especialmente entre as crianças e jovens de todo o mundo. Esta comemoração

[34] https://www.internetsegura.pt/publicacoes - Final Public Report | Portuguese Safer Internet Centre III | anuary 1st 2015 – June 30th 2016

envolve mais de 100 países de todos os continentes. Em Portugal, em 2017 esta comemoração envolveu mais de 217.000 participantes em cerca de 8.500 escolas envolvidas de 60 municípios distintos.

- Sessões de sensibilização nas escolas: Os Centros de Competência TIC compreendem, ao momento, dez instituições que resultam de protocolos estabelecidos entre o Ministério da Educação e as entidades nas quais estes se encontram integrados. Estes centros dinamizam sessões de sensibilização nas escolas, onde se privilegia as ações junto de professores que por sua vez formarão os seus alunos. São realizadas cerca de 250 sessões de sensibilização (cerca de 30 000 participantes), por ano letivo.
- Dia da Defesa Nacional: iniciativa do Ministério da Defesa Nacional que conta com a participação da DGE, desde 2014. Cerca de 130 mil jovens com 18 anos participam numa sessão sobre cidadania digital (cerca de 900 sessões), no âmbito do projeto SeguraNet, compreendendo diversas temáticas, tais como: a proteção de dados, o *ciberbullying*, o *copyright*, a pegada digital, a reputação *online*, não ao discurso do ódio, a linhas de apoio-Linha Internet Segura e a linha de denúncia de conteúdos ilegais (apologia ao racismo, apologia à violência e abuso sexual de crianças) - Linha Alerta), entre outras.
- Iniciativas nas Escolas:
    - Desafios SeguraNet que já conta com a sua 11.ª edição e envolve em média 30 000 participantes por cada edição (entre professores, pais e alunos). São lançados Desafios dirigidos ao 2.º Ciclo e ao 3.º Ciclo que endereçam diversas temáticas da cidadania digital, no entanto existe uma categoria específica dirigida ao 1.º Ciclo;
    - Iniciativa Selo de Segurança Digital (*eSafety Label*) que visa promover e certificar práticas de segurança digital e sendo que Portugal é o segundo país com mais registos de Escolas nesta iniciativa, contando já com um selo de ouro, 4 selos de prata, 196 de bronze. A participação por parte das escolas implica o preenchimento de um questionário de autoavaliação, que será objeto de análise e sugestão de um plano de ação com melhoria. As escolas receberão um certificado (selo de bronze, prata ou ouro) face às melhorias efetuadas.
    - Recursos educativos Digitais: São diversos os recursos educativos digitais, entre eles, uma aplicação digital, comumente referida como *app*, dirigida ao 3.ºCiclo - Pisca Mega Quis; planos de aula dirigidos ao 3.ºCiclo - The Web We Want; jogo de cartas - Quiz4You SeguraNet; jogos *online*; cartazes (durante o ano corrente foi distribuída uma coleção de cartazes ”O Pisca não arrisca” a cerca de 8000 estabelecimentos do 1.º Ciclo e jardins de infância e a coleção “5 dicas” dirigida ao 2.º Ciclo foi distribuída a cerca 4000 escolas do 2.º Ciclo); árvores de decisão; origamis e folhetos informativos.

Por outro, e na vertente da integração dos conteúdos digitais no currículo escolar da disciplina de TIC, salienta-se que desde 2012 que esta disciplina contempla as questões relativas à segurança digital, também a disciplina da Educação para a Cidadania dispõe de referenciais e documentos alusivos à abordagem da educação para os *media* e por fim no âmbito do Projeto de Autonomia e Flexibilidade Curricular, cerca de 300 agrupamentos podem abordar estas temáticas nas aprendizagem essenciais das TIC.

Guarda Nacional Republicana (GNR)[35]

Segundo os autores, o objetivo principal da GNR com o desenvolvimento do projeto CyberGNRation é criar e instalar um espírito de segurança cibernética nos cidadãos, para que as novas gerações de utilizadores do ciberespaço estejam mais conscientes dos riscos inerentes ao uso da Internet. Este projeto de cibersegurança descreve o ponto de vista da GNR e as ações necessárias, com base na proteção e promoção dos direitos dos cidadãos, para tornar o ciberespaço um "lugar seguro para circular".

O contexto foi previamente analisado, através de bases de dados onde estão registados os incidentes criminosos. Posteriormente os dados existentes foram processados e compilados, dando especial destaque aos crimes relacionados ao uso da Internet.

		2014	2015	2016	2014/2015	2015/2016
Cibercrimes	Privacy abuse	70	83	102	13	19
	False information	7	7	3	0	-4
	Sabotage	0	2	4	2	2
	Scams	680	1 044	885	364	-159
	Other crimes	21	14	16	-7	2
	Total	778	1150	1010	372	-140
Crimes boosted by the use of the Internet	Other scams	2 528	2 880	3 169	352	289
	Extortion	61	76	99	15	23
	Other crimes against privacy	257	276	294	19	18
	Defamation, slander and insult	3 147	3 127	3 222	-20	95
	Sexual abuse of minors	136	115	109	-21	-6
	child pornography	28	13	18	-15	5
	Threat and coercion	7 161	7 124	6 688	-37	-436
	Simple physical offense	11 448	10 829	10 430	-619	-399
	Total	24766	24440	24029	-326	-411

Figura 2 – Dados de Cibercrimes relativos aos anos 2014, 2015 e 2016

A Internet é hoje o instrumento central no desenvolvimento do processo de globalização, no entanto, essa centralidade, ao mesmo tempo que torna possível a globalização, também traz riscos,

[35] Entrevista ao Major Paulo Poiares (Direção de Operações - Comando Operacional) no dia 6 de outubro de 2017

com implicações em todas as áreas – nomeadamente na segurança e na defesa nacional. Também a utilização da *darknet*[36] evoluiu significativamente nos últimos anos, principalmente por indivíduos isolados ou grupos criminosos que comercializam diversos tipos de produtos ilícitos e por outro lado, o crescimento exponencial de dispositivos conectados, dentro e além fronteiras, contribui para aumentar a complexidade dos ataques dirigidos contra uma única pessoa ou uma entidade e, consequentemente, para o aumento das possibilidades de vetores criadores de crime.

Todos os fatores apresentados anteriormente levaram a um aumento natural da criminalidade, conduzindo as forças de segurança a desenvolver estratégias policiais que contribuem para a redução das taxas de criminalidade e evitam a ocorrência de novas ciber ameças.

A intervenção da GNR na proteção da população inicia-se com a adequação do modelo policial, sendo este preponderante na forma com a GNR responde aos atuais desafios digitais. Por outro lado, os cidadãos devem manter as mesmas normas, princípios e valores *online* que mantém *offline*. Neste sentido os direitos fundamentais e o Estado de Direito também necessitam de proteção no ciberespaço.

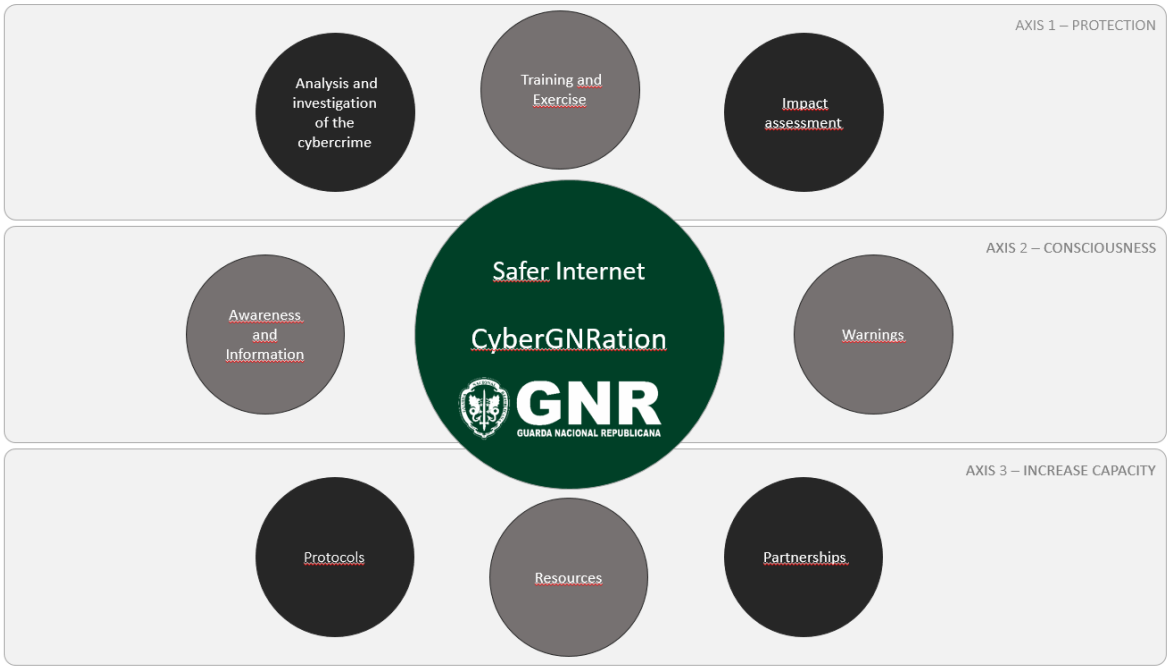

Figura 3 – Desenho estratégico do projeto Safer Internet - CyberGNRation

Os autores defendem que o projeto Safer Internet - CyberGNRation é relevante no contexto da Estratégia de Cibersegurança da UE, da Estratégia Nacional de Segurança do Ciberespaço e da Agenda Europeia de Segurança de 2015, porque descreve a visão e os princípios sobre a aplicação

[36] *Darknet* é uma rede fechada, usada por um grupo privado de pessoas com o intuito de comunicar. Desde 2002 que o termo evoluiu e atualmente refere-se às redes onde se partilha conteúdo de forma anónima, sendo impossível identificar o utilizador. Os ficheiros disponibilizados estão encriptados. A *darknet* é muitas vezes utilizada para partilhar informações sigilosas.

dos valores fundamentais da UE e dos direitos fundamentais no ciberespaço, permitindo a melhoria dos valores éticos e morais que devem ser tomados em conta pelo utilizador da Internet.

As linhas de ação identificadas são as seguintes: Análise e investigação do fenómeno do cibercrime – com o objetivo de realizar uma análise criminal do fenómeno, a fim de identificar os principais crimes relacionados com o uso da Internet e avaliar a evolução com o desenvolvimento e implementação do projeto; Formação e exercício - para que as ações preventivas sejam efetivas é necessário que o pessoal militar da GNR tenha a formação adequada, que lhes permita responder dentro do ciberespaço. Outro objetivo é realizar exercícios em conjunto com outras instituições com diferentes competências e responsabilidades na cibersegurança, permitindo simular situações de risco e identificar medidas para resolução de problemas comuns; Avaliação de impacto - medir e demonstrar o impacto social é crucial para validar as escolhas feitas e alinhar o próximo passo do projeto; Ações de sensibilização e consciencialização, sobre a prevenção da cibersegurança, dirigida aos cidadãos, especialmente aos jovens, promovendo a prevenção do cibercrime, fortalecendo os valores éticos a partir dos quais o ciberespaço deve ser construído. Um exemplo de ações de consciencialização já realizadas, e que envolve a comunidade escolar geral, é o envolvimento no Dia da Internet Mais Segura; Promoção da sensibilização dos jovens para o desenvolvimento cognitivo, iniciativa e espírito de inovação e sentido crítico sobre questões de cibersegurança e cibercrime e violações inerentes à Internet; Avisos - publicação contínua de conselhos sobre o uso das redes sociais, com o objetivo de alertar os cidadãos e evitar a sua exposição a situações negativas; Protocolos – o projeto implica a cooperação contínua com várias instituições, uma vez que a cooperação entre instituições e organizações no campo da Cibersegurança nacional e internacional viabilizam o aumento da capacidade da GNR, através do intercâmbio de conhecimentos; Recursos – a necessidade de desenvolver recursos para enfrentar as potenciais alterações sociais e enfrentar os desafios criados pelo ciberespaço e Parcerias – com o objetivo de transmitir a mensagem da GNR e alcançar o maior número possível de cidadãos.

O projeto consiste essencialmente em diferentes formas de redes de comunicação e iniciativas de participação conjunta (campanhas de conscientização, sessões de formação, competições, seminários, *webcasts*, etc.) para construir e consolidar valores éticos e morais entre todos os utilizadores do ciberespaço, especialmente nos jovens, para prevenir e reduzir o cibercrime, e aumentar o sentimento de segurança entre os cidadãos.

A indústria e as organizações terão um papel preponderante, pois estarão envolvidas (por exemplo, em exercícios e em oficinas promovidas pelas forças de segurança) numa perspetiva cooperativa, com o objetivo de identificarem as suas próprias preocupações em termos de cibercrime e transmitir essas preocupações às forças de segurança. Desta forma, as forças de segurança podem abordar melhor as iniciativas de prevenção da criminalidade e definir iniciativas de consciencialização para grupos de risco. Exemplos de competições já em curso e enquadrados neste âmbito são a "Carta dos Princípios de Cibersegurança", redigida por jovens em 2015 no âmbito do Projeto Internet Mais Segura e o desafio "CyberChallenge" que tem equipas de estudantes que são desafiadas por organizações diversas.

No âmbito destas ações de conscientização estão a ser estabelecidas parcerias com os conselhos locais e as organizações da sociedade civil, de modo a garantir que as Seções do Programa Especial GNR tenham os recursos necessários para realizar as ações de conscientização. Os idosos e os lares de idosos serão contactados pessoalmente para participar nas campanhas de conscientização

Em forma de conclusão, no campo de ação deste projeto serão realizadas várias iniciativas de mobilização a nível nacional. O foco serão os cidadãos que estão envolvidos em programas de prevenção relacionados com o cibercrime, especialmente relacionados com as atividades criminosas que são conduzidas, cada vez mais, na Internet, sendo o objetivo final a redução da criminalidade, reforçando a "cidadania digital".

Instituto de Informática, I.P[37]

O Instituto de Informática, I.P. (II, I.P) tem como missão primordial definir e propor políticas e estratégias TIC, que garantam o planeamento, a conceção, a execução e por fim a avaliação das iniciativas de informatização e de atualização tecnológica do Ministro do Trabalho, Solidariedade e Segurança Social (MTSSS).

Neste âmbito, o II, I.P. atualmente, possui um plano de comunicação de segurança da informação que envolve diversas atividades, das quais se destaca o curso de E-Learning “Segurança na ponta dos dedos”. Este curso teve como objetivo principal sensibilizar todos os colaboradores do Instituto de Informática – Internos e externos, no entanto, posteriormente ocorreu o alargamento aos organismos do Ministro do Trabalho, Solidariedade e Segurança Social (MTSSS). Esta sensibilização foca-se no tema da cibersegurança, promovendo uma cultura transversal em todos os domínios de atuação, tanto pessoal como profissional, procurando reduzir o risco de exposição a um conjunto alargado de ameaças, tal como a engenharia social, o *phishing*, o *malware*, entre outras.

Das ações identificadas no programa de atuação do II, I.P. é de salientar o curso E-Learning “ABC de Segurança da Informação”, que se foca principalmente no reforço nas atividades diárias no âmbito dos processos de trabalho do MTSSS; a comunicação via Intranet, a Comunicação via WebLetter e as Sessões de Esclarecimento e Informação (SEIs) que são presenciais e temáticas.

Este plano de comunicação tem como objetivo comunicar de forma efetiva, a todas as partes interessadas, temas relevantes da segurança da informação, devidamente enquadrados, reforçando a cultura organizacional de segurança, tanto na vertente de cibersegurança como na proteção de dados.

[37] Entrevista ao Engenheiro Nuno Miranda - Diretor de Segurança de Informação, no dia 3 de outubro de 2017

Figura 4 –Curso de E-Learning – Segurança na ponta dos dedos do II, I.P

No que diz respeito à avaliação deste curso, a taxa de participação global, tando de formandos internos como externos foi de 64%, tendo o teste final de avaliação dos conhecimentos tido um resultado médio 89,7%.

Nesta dissertação optamos por destacar apenas alguns, entre os inúmeros programas de capacitação de cidadãos, espalhados geograficamente. Salienta-se que todos eles têm especificidades próprias do país onde estão integrados e são dirigidos a públicos distintos.

Confrontando os programas de capacitação aplicados a cidadãos nacionais e o Relatório Anual de Segurança Interna de 2016[38], conclui-se que em matéria de sensibilização para os desafios digitais ainda muito há a fazer.

Neste sentido, globalmente em 2016, os ciberataques aumentaram exponencialmente, tanto em número, como em sofisticação e mesmo em consequências. Portugal, não foi exceção e os crimes informáticos mantêm a tendência de subida, tendo sido registados 142 casos o que se traduz num aumento de 21,5%.

[38] RASI 2016 - http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20(RASI)/RASI%202016.pdf - consultado em 13 de outubro de 2017

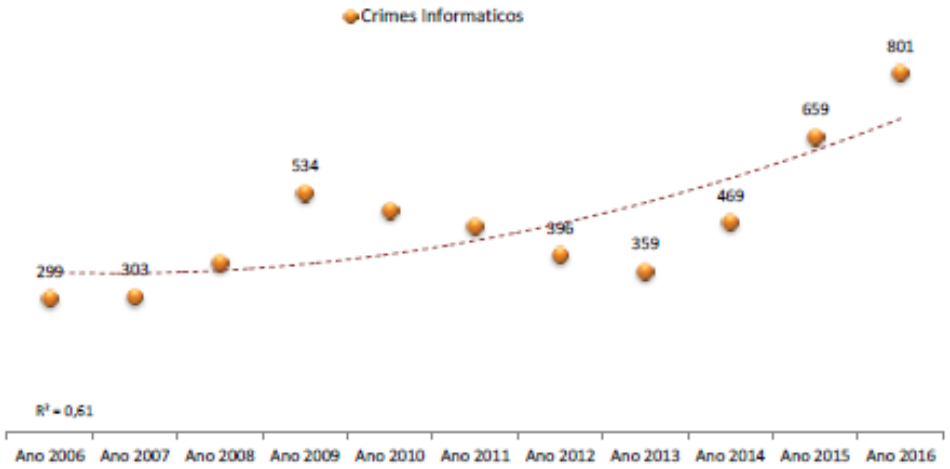

Figura 5 - Dados relativos a crimes informáticos[39]

Relativamente à criminalidade informática praticada, fazendo uso de tecnologia informática, ocorreu em 2016 um aumento significativo do crime de sabotagem informática (140%), programas informativos (121%) e falsidade informática (58%), relativamente a 2015. Os crimes de extorsão, vulgo *ransomware*, também registaram uma tendência crescente em 2016 e em 2017, ainda sem dados oficiais e sem o ano terminado, o panorama foi bastante expressivo, com os ataques de abrangência generalizada, WannaCry[40], Not Petya[41] e Bad Rabbit[42].

Segundo dados do RASI de 2016, em Portugal registou-se um crescimento do *ransomware* e uma estabilização do uso de moedas virtuais. Por outro lado, prevê-se que os dados pessoais venham a constituir uma área crescente de crime. Sugere este relatório, nomeadamente na área da prevenção criminal, uma maior intervenção na sensibilização através de diversas parcerias e em articulação com diferentes campanhas e organismos e também através da divulgação em redes sociais com intervenção direta sobre os públicos alvo.

[39] Crimes informáticos: acesso indevido/ilegítimo, falsidade informática, outros crimes informáticos, reprodução ilegítima de programas protegidos, sabotagem informática, viciação ou destruição de dados/dano relativamente a programas

[40] WannaCry é um *crypto-ransomware* que afeta o sistema operativo Windows e cuja difusão em larga escala ocorreu a 12 de maio de 2017 através de técnicas de phishing, infetando mais de 230.000 sistemas mundialmente.

[41] Not Petya é um *malware*, cuja variante voltou a causar danos em junho de 2017 e fez mais de dois mil ataques em todo o mundo, tendo sido a Rússia e a Ucrânia os países mais afetados.

[42] "Bad Rabbit" foi o mais recente *crypto-ransomware* (outubro de 2017). Da mesma forma que WannaCry, Bad Rabbit cifra documentos do Windows, vídeo e áudio.

4. Políticas Públicas em Cibersegurança

Os Estados e as organizações incluem nas suas dinâmicas quotidianas o uso das TIC pelos cidadãos, facto pelo qual se tem assistido à promoção da melhoria e sensibilização contínua de planos de ação e coordenação nas áreas da cibersegurança.

É desta forma imperativo que os Estados respondam eficazmente aos desafios que lhes são colocados, pela evolução e pela dependência das sociedades atuais relativamente à informação e pela necessidade de garantia da segurança e da disponibilidade dos serviços críticos que alicerçam estas mesmas sociedades e informações, quase sempre suportadas, de forma direta ou indireta, em infraestruturas e processos tecnológicos.

Não podemos considerar a necessidade de segurança sem considerarmos a importância e o determinante predomínio do fator humano na sua promoção e efetivação. São realmente as pessoas o principal ativo das sociedades e foi em benefício das mesmas que a humanidade evoluiu a favor da inovação e do desenvolvimento tecnológico, colocando-nos no patamar atual da evolução, mas, e talvez principalmente, de dependência tecnológica

Atualmente os cidadãos têm cada vez mais acesso a dispositivos tecnológicos que potenciam inegáveis vantagens na melhoria da qualidade de vida, mas, por outro lado, trazem problemas e dilemas em relação à garantia dos direitos e liberdades fundamentais que demoraram séculos a edificar e que, de uma forma simples e eficaz, poderão ser colocados em causa através da tecnologia que foi desenvolvida para os potenciar e defender. Ao longo dos últimos anos fomos constatando que existe um défice relativamente às capacidades dos equipamentos tecnológicos desenvolvidos e as competências das pessoas que fazem uso dos mesmos, ou são visadas, pelas potencialidades desses mesmos equipamentos. Pensar em Segurança da Informação sem considerar que as pessoas são parte da equação do sucesso que produz essa mesma segurança, tem sido um dos vazios identificados pelos atores envolvidos nestas temáticas.

Os Estados e principalmente as organizações têm um papel fundamental, e simultaneamente catalisador, no desenvolvimento das sociedades e na promoção da inovação tecnológica, tendo sempre que tomar em consideração que os cidadãos necessitam de competências e de sensibilização para que possam acompanhar a evolução da tecnologia. É de realçar que é para benefício das sociedades que a tecnologia é desenvolvida e é apenas através do benefício das sociedades que as organizações prosseguem o seu caminho em direção ao desenvolvimento da utilidade, eficiência e segurança da tecnologia.

4.1. Estratégia Nacional de Segurança do Ciberespaço (ENSC)

Em 28 de maio de 2015 foi aprovada pela Resolução do Conselho de Ministros n.º 36/2015 a Estratégia Nacional de Segurança do Ciberespaço, visando o compromisso de aprofundar a segurança das redes e da informação, garantindo a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciando uma utilização livre, segura e eficiente do Ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas. A ENSC alicerçou-se nos princípios gerais da soberania do Estado, nas linhas gerais da Estratégia da União Europeia para a

Cibersegurança e na Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, da liberdade de expressão e do respeito pelos dados pessoais e privacidade.

O desenvolvimento da capacidade nacional em matéria de Cibersegurança, bem como a responsabilidade do Estado na operacionalização da coordenação nacional nesta matéria, são as principais orientações políticas e estratégicas da ENSC.

A ENSC estabelece ainda quatro objetivos estratégicos, que podemos consolidar em "*promover uma utilização consciente, livre, segura e eficiente do ciberespaço; proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação*". Para que possam ser alcançados os objetivos acima referidos, são definidos na ENSC seis eixos de atuação (Estrutura de segurança do Ciberespaço; Combate ao cibercrime; Proteção do Ciberespaço e das infraestruturas; Educação, sensibilização e prevenção; Investigação e desenvolvimento; Cooperação), a implementar segundo os princípios da Subsidiariedade, Complementaridade, Cooperação, Proporcionalidade e Sensibilização.

Figura 6 - Eixos de atuação, princípios e objetivos da ENSC.

No âmbito do presente trabalho o eixo quatro tem especial relevância uma vez que considera que "*o sucesso da segurança do ciberespaço passa pela promoção de uma cultura de segurança que proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização dos sistemas de informação*" e, na mesma linha de importância, defende como fundamental "*que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço*".

Ora neste sentido e respondendo ao desafio do eixo da Educação, sensibilização e prevenção (e focando-nos apenas no termo sensibilização) fará todo o sentido implementar um programa de sensibilização de cidadãos. A este programa poderemos chamá-lo de um programa de *Cyber Hygiene* (Ciber higiene*)*, cujo princípio fundamental se centra na segurança da informação por analogia à higiene pessoal, isto é, o equivalente a rotinas simples que minimizem os riscos de ameaças de cibersegurança. Parte-se então do pressuposto que a aplicação de boas práticas de ciber-higiene pode propulsionar a imunidade crescente e desejável das organizações às ameaças do ciberespaço, reduzindo o risco a que as mesmas estão sujeitas. As abordagens típicas de um programa desta ordem devem abranger principalmente as seguintes áreas: Proteção do perímetro, proteção da rede, proteção dos dispositivos individuais, usar a nuvem de forma segura e proteção da cadeia de valor da organização (ENISA - European Network and Information Security Agency, 2016).

4.2. InCode2030

Ciente de que Portugal deve diligenciar a criação de novas competências digitais orientadas para o futuro e para as novas oportunidades que emergem a cada dia, o XXI Governo da República Portuguesa, no âmbito do Programa Nacional de Reformas, lançou a Iniciativa Nacional em Competências Digitais e.2030 (Republica Portuguesa- XXI Governo, 2017). Este é um programa integrado de competências digitais, que pretende que Portugal responda a três principais desafios, entre 2017-2030, nomeadamente "*Garantir a literacia e a inclusão digitais para o exercício pleno da cidadania, Estimular a empregabilidade e especialização em tecnologias e aplicações digitais para a qualificação do emprego e uma economia de maior valor acrescentado, e Produzir novos conhecimentos nas áreas digitais em cooperação internacional*".

A crescente exigência das competências digitais para o exercício de diferentes profissões obriga a que na população ativa, variáveis como a aprendizagem, a produtividade e a competitividade estejam cada vez mais dependentes das TIC. Ainda relativamente às competências digitais, e tomando como referência o índice Digital Economy & Society Index (DESI) da Comissão Europeia (Comissão Europeia, 2017), Portugal situa-se no décimo quinto lugar (15º), ou seja, exatamente na mediana europeia (Figura 3), necessitando assim de robustecer as competências básicas em Tecnologias de Informação e Comunicação (TIC), principalmente no que se refere ao capital humano e aos níveis de utilização da Internet.

Neste campo existe um grande potencial na requalificação de indivíduos que possam responder às exigências da oferta de emprego típica das sociedades modernas, como é a nossa, a portuguesa. A requalificação tem neste programa uma função exigente e que obriga a uma mobilização e uma combinação de esforços das diferentes áreas da governação e da sociedade civil.

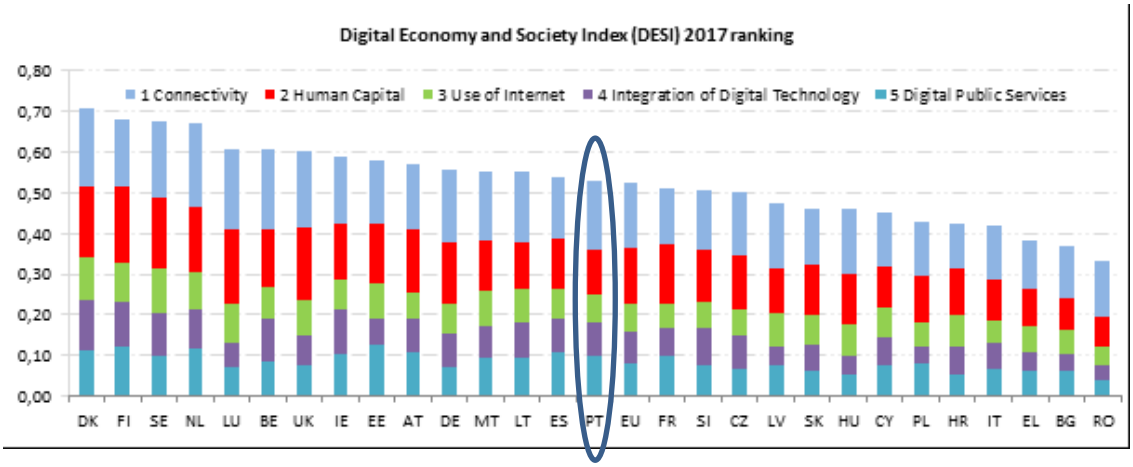

Figura 7 - The Digital Economy and Society Index (DESI) - DESI2017

Seguindo este raciocínio criar uma sociedade mais resiliente implica assim despertar para novas competências, especialmente digitais, que estão em contínua mudança e evolução, e simultaneamente exige uma melhor preparação da população para a crescente incerteza, admitindo que existem desigualdades que impõem modelos de preparação diferenciados.

Capacitar os cidadãos em competências digitais[43] consiste num estímulo e num desafio para o interesse intelectual e económico de muitos atores do mercado. Neste sentido, e para apoiar estes atores, a iniciativa materializa (através do Programa Nacional de Reformas) vários objetivos, tais como a inclusão e a literacia digital, a garantia do acesso físico e cognitivo de todos os cidadãos aos serviços públicos digitais, a capacitação analítica para a sociedade e a economia em contexto de grande volume de dados, a produção e a divulgação de informação, a privacidade e a segurança, a utilização das tecnologias de informação, comunicação e eletrónica nos processos de ensino e aprendizagem ao

[43] Por Competências Digitais, assumiu este programa integrado de competências digitais para Portugal, 2017-2030, um âmbito abrangente e que inclui a noção de literacia digital (i.e., da capacidade de aceder aos meios digitais e às TIC, para compreender e avaliar criticamente conteúdos, bem como comunicar eficazmente), e a investigação e produção de novos conhecimentos. Este conceito baseia-se num quadro de referência suportado em cinco domínios: O processamento de informação, em que se considera a utilização das tecnologias digitais para navegar, procurar, extrair e filtrar informação, avaliá-la e armazená-la; A comunicação e colaboração, em que se considera a utilização de canais digitais para interagir com outros usando diferentes tecnologias, partilhar informação e conteúdos; O desenvolvimento de conteúdos digitais, tendo em atenção o respeito pelos direitos de propriedade intelectual e a sua defesa e preservação; A segurança e privacidade, em que se considera a proteção de dispositivos e dados pessoais, bem como a preservação das questões de saúde e das condições ambientais; E finalmente, o uso das tecnologias digitais para a conceção de novas soluções para problemas de natureza muito diversa, pela integração de conhecimento interdisciplinar e análise de dados, pela utilização intensiva de inteligência artificial, pelo recurso a instrumentação avançada e a redes de comunicação e sistemas móveis, pelo desenvolvimento de sistemas ciberfísicos e sua programação, envolvendo judiciosamente hardware e software e alargando o conceito das TIC à eletrónica, automação e robótica.

longo de toda a vida, assim como atividades de investigação e desenvolvimento orientadas para a produção de novos conhecimentos e formas avançadas de computação científica.

A iniciativa Portugal INCoDe.2030 pretende implementar várias medidas que têm como objetivo mobilizar os diversos organismos do Estado em articulação com as iniciativas convergentes da sociedade civil. As medidas propostas estão organizadas em cinco eixos principais de ação: Inclusão, Educação, Qualificação, Especialização e Investigação. Destacamos o eixo da Inclusão e da Qualificação por consideramos que o desenvolvimento do nosso trabalho e em particular do futuro programa de capacitação se enquadra perfeitamente nestes dois eixos. Por definição, o eixo da Inclusão pretende "assegurar a generalização do acesso às tecnologias digitais a toda a população, para obtenção de informação, comunicação e interação" e o da Qualificação, pretende "capacitar profissionalmente a população ativa munindo-a dos conhecimentos necessários à integração no mercado de trabalho que depende fortemente de competências digitais.

Ainda neste âmbito e na perspetiva dos desafios, foram definidos 4 (quatro) grandes desafios societais, sendo que salientamos o primeiro deles uma vez que no campo de ação deste trabalho é aquele onde consideramos poder caber o programa de capacitação de cidadãos que nos propomos desenvolver – "*generalizar a literacia digital, com vista ao exercício pleno de cidadania e à inclusão numa sociedade com práticas cada vez mais desmaterializadas, e em que muitas interações sociais acontecem na Internet e são crescentemente mediadas por dispositivos eletrónicos*".

Usar as TIC com competência e segurança tornou-se num instrumento de inclusão social e essencial para o exercício pleno da cidadania. É necessário ultrapassar várias barreiras e limitações dos cidadãos para que, de um modo generalizado, os mesmos possam beneficiar das tecnologias digitais. Neste sentido, a iniciativa INCoDe.2030 pretende responder a este repto, desenvolvendo competências digitais enquadradas nos seguintes objetivos: Promover novas competências digitais na administração pública e na interação com os cidadãos; Criar um quadro dinâmico de referência de competências digitais específico para a administração pública tendo por base a evolução contínua de quadros de referência Europeus já existentes; Promover e manter um sistema *online* de autodiagnóstico das competências digitais dos trabalhadores em funções públicas; Promover a qualificação digital dos trabalhadores em funções públicas, e, consequentemente, a capacidade da administração pública para melhorar e modernizar os serviços públicos. Focando-nos no projeto a que nos propomos neste trabalho - capacitação de cidadãos em cibersegurança, pensamos ter enquadramento viável, no primeiro destes objetivos - promoção de novas competências digitais na administração pública e na interação com os cidadãos, bem como no terceiro objetivo - promoção e manutenção um sistema *online* de autodiagnóstico das competências digitais dos trabalhadores em funções públicas, neste caso particularizando nas competências digitais em cibersegurança.

4.3. SIMPLEX +

O programa de simplificação administrativa e legislativa - Simplex - tem com objetivo primordial facilitar a vida dos cidadãos e das empresas no relacionamento com a Administração Pública, contribuindo desta forma para o aumento da eficiência interna dos serviços públicos. O programa visa

alterar processos e simplificar e/ou eliminar procedimentos pouco eficientes que se encontrem inseridos nas leis e regulamentos que agora vigoram.

A gradual exigência dos cidadãos, com mais informação, mais exigentes e preocupados com a qualidade dos serviços públicos e, obviamente mais dispostos a se envolverem na sua transformação, mencionando e expondo, se necessário, as falhas e as oportunidades de melhoria, é uma das principais motivações por parte do Governo para a criação do programa Simplex.

Desde 2006 que o programa Simplex tem permitido a apresentação de várias medidas de simplificação com impactos positivos na vida dos cidadãos e das empresas, como são exemplo o cartão de cidadão, a empresa na hora, a informação empresarial simplificada ou o licenciamento zero. Durante alguns anos o programa esteve interrompido e regressou em 2016, com especial ímpeto na transformação digital dos serviços públicos.

Em 2017, o Governo lançou mais uma edição do Simplex+ e acrescentou-lhe novas ideias ao conjunto de iniciativas já implementadas e em curso, sendo que o Centro Nacional de Cibersegurança, enquanto organismo cuja missão é "*contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional*" (Presidência do Conselho de Ministros, 2014), tem um papel preponderante na dinamização de medidas relacionadas com a cibersegurança cujos destinatários sejam os cidadãos. Neste sentido, foi inscrita a medida - Portal do Centro Nacional de Cibersegurança. Esta medida tem como objetivo promover a partilha de conhecimentos na área da segurança digital, o desenvolvimento de novos conteúdos e recursos dedicados à educação, sensibilização e prevenção para a segurança e literacia digital e a promoção e utilização segura das TIC e da redução à exposição aos riscos no ciberespaço, dando particular importância à capacitação de cidadãos.

Refletindo sobre esta medida (#36[44]) consideramos que o trabalho que nos propomos desenvolver - Capacitação de Cidadãos em Cibersegurança, tem um enquadramento perfeito na medida inscrita no programa SIMPLEX + 2017.

4.4. Estado da União 2017

No passado dia 13 de Setembro de 2017, o Presidente da Comissão Europeia, Jean-Claude Juncker, proferiu o discurso sobre o Estado da União 2017 no hemiciclo do Parlamento Europeu, em Estrasburgo. Neste discurso, Juncker apresentou as suas prioridades para o próximo ano, expôs a sua visão da forma como a União Europeia poderá evoluir até 2025, apresentou o Roteiro para uma União Mais Coesa, Mais Forte e Mais Democrática e, sob o tema da cibersegurança, afirmou: "*Nos últimos três anos, fizemos progressos para garantir a segurança dos cidadãos europeus na Internet. Contudo, ainda não estamos suficientemente preparados para fazer face a ciberataques. A Comissão propõe hoje a adoção de novos instrumentos, nomeadamente a criação de uma Agência da União Europeia para a Cibersegurança, para nos defender melhor desse tipo de ameaças*."

[44] (AMA - Agência para a Modernização Administrativa, I.P., 2017)

Neste sentido, e para que a Europa esteja munida de apropriados instrumentos para lidar com os ciberataques, a Comissão Europeia (CE) propuseram algumas medidas destinadas a fortalecer a área da cibersegurança na UE, designadamente com a proposta de criação de uma Agência da UE para a Cibersegurança, com o objetivo de apoiar os Estados-Membros a responderem adequadamente aos ciberataques, bem como com um novo sistema europeu de certificação que avalize e certifique que os produtos e serviços no mundo digital utilizados no espaço da UE são seguros.

Os mais recentes dados evidenciam que as ciberataques estão a evoluir aceleradamente, sendo que desde o início de 2016, já ocorreram mais de 4.000 ataques de *ransomware*, o que se traduz num aumento de 300% desde 2015. São também relevantes os indicadores que demonstram que 80% das empresas europeias foram alvo de um ciberataque em 2016.

O considerável aumento da cibercriminalidade, os recentes ataques de *ransomware*, o cada vez mais acentuado uso de ferramentas TIC e a diversificação dos incidentes de cibersegurança, levou assim a uma tomada de posição em matéria de cibersegurança, de modo a que a UE se torne mais resiliente aos ciberataques e crie uma dissuasão eficiente e uma pronta resposta (estratégica, operacional, técnica e legislativa) que proteja os cidadãos, as empresas e as instituições públicas.

Posteriormente, e passando do discurso aos atos, a Comissão divulgou um amplo pacote de cibersegurança que visa equipar a Europa com as ferramentas certas para responder assertivamente aos ciberataques.

Reforçar a resiliência da UE através da criação de uma Agência da UE para a Cibersegurança foi a ponto basilar das medidas a por em prática. A nova Agência terá um mandato permanente para ajudar os Estados-Membros a prevenirem e a responderem eficazmente aos ciberataques e terá na sua génese a atual Agência da União Europeia para a Segurança das Redes e da Informação (ENISA). Entre outros, terá como objetivo melhorar a preparação da UE na reação a incidentes de cibersegurança, através da organização anual de exercícios europeus de cibersegurança e através da criação de centros de partilha e análise de informações, como forma de garantir uma partilha de informação e conhecimento sobre ameaças.

Figura 8 - Resultado gráfico do Survey 2016 Report- Marsh[45]

Reforçamos ainda que na folha informativa (European Commission, 2017) sobre a resiliência da UE relativamente aos ciberataques é mencionado que, apesar da crescente ameaça, a consciencialização e o conhecimento dos cidadãos para as questões de cibersegurança são ainda insuficientes.

[45] Continental European Cyber Risk Survey: 2016 Report (Marsh, 2016)

Este sinal de reconhecimento político, ao mais alto nível, de que a cibersegurança é hoje estrategicamente relevante, as opções estratégicas enunciadas e a referência à falta de consciencialização e conhecimento dos cidadãos para as matérias de cibersegurança, reforçam a confiança e o investimento de que o trabalho aqui proposto - a criação de um programa de capacitação em cibersegurança, terá o acolhimento e a implementação desejados junto dos cidadãos, que Portugal e a Europa da era digital necessitam para se tornar mais resiliente.

5. Programa de capacitação de cidadãos em cibersegurança

O desenvolvimento de um programa de capacitação em cibersegurança não é mais do que um programa de ciber-higiene que contribuirá, entre outros, para a redução do número de incidentes de cibersegurança que ocorrem por falta de consciencialização dos cidadãos para estes temas.

Uma forma aliciante de informar os cidadãos e os trabalhadores sobre as atividades maliciosas que ocorrem no ciberespaço e que visam as organizações onde os mesmos trabalham, é convidá-los a participar num programa de capacitação em cibersegurança.

Organizações com estratégias de segurança holística, que integram ferramentas, processos, políticas e trabalhadores capacitados nas temáticas dos ciberincidentes, reconhecem com mais facilidade uma potencial ameaça, reportando-a sempre que se cruzarem com atividades suspeitas. A consciencialização dos trabalhadores é, assim, um elemento chave para uma implementação bem-sucedida de qualquer programa de capacitação em cibersegurança

Na revisão da literatura efetuada encontramos detratores (Masadeh, 2012) de programas de capacitação de cibersegurança que defendem que, independentemente da preparação e formação que os utilizadores recebam, os incidentes continuarão a ocorrer, uma vez que o elemento humano é um dos elos mais fracos da cadeia de cibersegurança. Estes também defendem que há uma desconexão entre o desempenho dos utilizadores e a capacidade de reconhecer ameaças em ambiente de exercício, isto é, quando esperam vir a ser testados alteram os seus comportamentos e respostas em ambiente de vida real.

Todavia, nós acreditamos que vale a pena investir em programas de capacitação e de formação de cidadãos e trabalhadores em cibersegurança. Qualquer cidadão necessita de estar ciente das ameaças mais comuns, de modo a que nem o próprio nem a organização onde trabalha, sejam vítimas dos incidentes mais simples, como por exemplo de *phishing*. E no caso de ataques de cibersegurança mais sofisticados, estes utilizadores podem, pelo menos, aplicar os conhecimentos adquiridos durante o programa de capacitação para mitigar os efeitos do incidente e informar o departamento/equipa apropriada para a resposta e o tratamento do incidente. Para a promoção de uma cultura consciente de cibersegurança, para reduzir riscos e prevenir ameaças de cibersegurança as organizações dependem dos seus trabalhadores.

Tipicamente quando se trata de um programa de capacitação de cibersegurança para uma organização específica, deve ser tomado em consideração que o programa pode e deve ser adaptado às necessidades dos trabalhadores, isto é, deve ser efetuada uma avaliação para identificar riscos e impactos de ataques de cibersegurança, métodos de consciencialização preferenciais, estratégias de reforço e medidas que avalizem o cumprimento dos objetivos de cibersegurança e a avaliação periódica do programa. Particularizando no objeto de análise deste trabalho - um programa de capacitação de cibersegurança generalista e potencialmente aplicado aos cidadãos comuns e aos trabalhadores de qualquer organização ou organismo da Administração Pública - também poderemos efetuar uma avaliação que efetue a identificação genérica e abrangente dos riscos e dos impactos dos ataques de cibersegurança, dos métodos de capacitação preferenciais para a generalidade dos cidadãos

abrangido, das estratégias de reforço e das medidas que avalizem o cumprimento dos objetivos de cibersegurança e a avaliação periódica deste programa.

O desenvolvimento do programa de capacitação em cibersegurança envolve três etapas principais: planear o programa de capacitação, desenvolver o material de sensibilização e implementar o programa. No entanto, criar uma sociedade mais resiliente implica despertar para novas competências, especialmente digitais, que estão em contínua mudança e evolução, pelo que também este programa estará em constante atualização e mutação, o que se reflete também nas etapas a percorrer.

5.1. Planear, desenvolver e implementar um programa de capacitação em cibersegurança

5.1.1. Planear

Os programas de capacitação em cibersegurança devem ser planeados tendo em consideração a organização e o seu ecossistema. No caso particular do programa de capacitação de cibersegurança que nos propomos desenvolver, temos em mente a atribuição dada ao CNCS de "*promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança*".

Neste sentido, o programa deve suportar as necessidades nacionais relativamente ao incremento das competências digitais em matérias de cibersegurança e ser relevante para a cultura digital de Portugal e das suas organizações. Tipicamente, os programas de capacitação bem-sucedidos, são aqueles em que os utilizadores se sentem que fazem parte da solução, isto é, que são relevantes no sucesso dos assuntos e das questões apresentadas.

5.1.2. Desenvolver

Ao iniciar o desenvolvimento dos conteúdos, a pergunta que se impõe e que deve ser respondida em primeira instância é: Qual o comportamento que pretendemos fortalecer?

Posteriormente devem-se desenvolver conteúdos adequados às necessidades do cidadão, ou seja, se o participante sentir que os conteúdos foram desenvolvidos para si, o participante dedicar-se-á e incorporará o que vir e ouvir no curso. Por outro lado, se o conteúdo for impessoal e demasiado genérico o programa será entendido como uma obrigação e não terá o resultado em termos de consciencialização pretendido. Concluindo, um programa de ciber-higiene terá um grau de eficácia superior se os conteúdos e as abordagens aos mesmos forem atuais, interessantes e relevantes.

Pelo facto do programa de capacitação em cibersegurança ser destinado aos cidadãos, os participantes das organizações poderão ser quaisquer uns, isto é, poderão ser todos os trabalhadores com contrato sem termo, contratados a termo certo ou outros trabalhadores da organização sem levar em linha de conta a hierarquia, a função ou o género. No entanto, a mensagem a ser disseminada através do programa de capacitação deverá ser distinta em função das responsabilidades do participante no tratamento da informação.

5.1.3. Implementar

No caso da aplicação do programa de capacitação em cibersegurança em organizações, este deve ser claramente explicado para que a organização obtenha suporte na implementação e o empenho dos recursos necessários. Este esclarecimento aos envolvidos deve incluir expectativas de gestão e de organização do programa, resultados esperados e benefícios para a organização. É essencial que todos os envolvidos na implementação do programa compreendam os seus papéis e responsabilidades. Também os horários e os requisitos de conclusão devem ser comunicados. Após o esclarecimento (e eventual aceitação) pelos decisores da organização, a implementação poderá ser iniciada e, neste caso particular, as organizações poderão adaptar a implementação do programa de capacitação em cibersegurança à sua dimensão, organização e graus de complexidade da sua organização.

Por outro lado, se o participante for um cidadão voluntário, nenhum dos requisitos anteriores é aplicável, pois parte-se do princípio que o mesmo tem consciência do nível de envolvimento que vai ocorrer, bem com da expectativa relativamente aos requisitos de conclusão. Também a implementação, isto é, a frequência de módulos, pode ser efetuada ao seu ritmo, dentro das limitações do próprio programa e do cidadão.

5.1.4. Após implementar

Com os frequentes e enormes avanços tecnológicos, com as transformações de infraestrutura de TI, com as mudanças organizacionais, entre outros, o programa de capacitação de cidadãos em cibersegurança pode tornar-se rapidamente obsoleto se não for dada especial atenção aos fatores referidos. Deste modo, torna-se necessário que o programa de capacitação integre mecanismos estratégicos que garantam a continuidade do programa relativamente á adequação e à pertinência dos conteúdos, às ferramentas e metodologias usadas, entre outras.

A melhoria contínua é um tópico que também deve ter um tratamento especial no seio do programa de capacitação de cidadãos em cibersegurança, uma vez que esta é uma área onde nunca se faz suficiente. Os esforços para apoiar o ciclo de *feedback* do após implementação devem ser desenvolvidos, sendo de considerar a satisfação do utilizador relativamente ao objetivo de melhoria contínua e de promoção da confiança.

5.1.5. Acompanhar a conformidade

Após a implementação do programa, paralelamente devem ser realizados processos de monitorização da conformidade e eficácia. Preferencialmente deve ser implementado um sistema de informação acoplado ao programa de capacitação, que recolha dados sobre a atividade do programa, nomeadamente sobre os cursos, módulos, conteúdos, datas, público a que se dirige, custos, entre outros. Um exemplo da pertinência deste sistema será por exemplo a identificação, numa organização, dos funcionários que necessitam de reciclar conhecimentos sobre cibersegurança.

Após a recolha da informação relevante, este sistema deve produzir análises e relatórios relativos à performance da iniciativa de ciber-higiene implementada. O acompanhamento da conformidade do programa envolve a avaliação do estado do mesmo, ajustando-o aos padrões inicialmente estabelecidos e, se necessário, identificando necessidade de ajustamento dos próprios

padrões. As lacunas e os problemas serão identificados através dos relatórios, que poderão ou não despoletar ações corretivas e ou de acompanhamento.

5.1.6. Avaliação e *Feedback*

Enquadrado na melhoria contínua, os mecanismos formais de avaliação e de comunicação de resposta, comumente apelidado de *feedback,* são tipicamente componentes críticos de qualquer programa de capacitação de cidadãos e que carecem de uma "dose" ajustada de bom senso.

Um programa de ciber-higiene pode ter variados mecanismos de avaliação e de *feedback*, nomeadamente *quizz*[46], formulários de avaliação, testes de escolha múltipla, testes de análise de comportamentos, observação independente, entrevistas, entre muitos outros. No caso do nosso programa de capacitação consideramos que o mais ajustado é a avaliação através da utilização de *quizz* intermédio com relatório de melhoria contínua e, posteriormente, *quizz* final com avaliação final do nível de conhecimentos adquiridos.

O programa que nos propomos implementar deve ter uma estratégia de comunicação de resposta que incorpore elementos como a qualidade do programa, o âmbito do programa, do curso e do módulo, o método de implementação, o nível de dificuldade, a usabilidade, a duração, a relevância, e sugestões de modificação.

As métricas são também de extrema pertinência na avaliação e comunicação de resposta, preferencialmente para medir a eficácia do programa de capacitação em cibersegurança, fornecer indicadores sobre o progresso e identificar áreas que carecem de melhoria.

5.1.7. Gerir a mudança

Tal como referido no ponto 5.1.4 - Após implementar, é necessário garantir que o programa de capacitação em cibersegurança continue a evoluir, acompanhando o ritmo da emergência de novas tecnologias, novas ameaças, novas soluções e eventualmente novos comportamentos associados. As necessidades de capacitação modificar-se-ão à medida que novas competências e capacidades forem necessárias para responder às novas mudanças digitais. Por outro lado, mudanças nas orientações e nos quadros de referência digitais, novas leis e decisões judiciais também podem impactar em novas ideias adaptadas às soluções de capacitação e conteúdo. Neste sentido, à medida que as políticas públicas de cibersegurança evoluem, também a oferta de capacitação deve evoluir e refletir essas mudanças.

5.1.8. Indicadores de sucesso do programa

O Governo, o Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança e a equipa envolvida no programa de capacitação em cibersegurança para cidadãos devem ser os principais defensores do programa que nos propomos desenvolver. Garantir a informação e a infraestrutura da organização deste programa é um esforço de equipa, que exige a entrega ao projeto de colaboradores dedicados.

[46] Quizz – teste de avaliação de conhecimentos ou comportamento efetuado em ambientes de aprendizagem.

Consideramos que alguns dos indicadores-chave para avaliar a aceitação, suporte e continuidade do programa, são os seguintes: as partes interessadas e os intervenientes demonstram comprometimento e apoio; o financiamento orçamentado está disponível para implementar o programa de capacitação em cibersegurança; equipa coesa e com conhecimentos adequados; infraestrutura robusta para o alojamento do programa e para a publicação de materiais diversificados; forte promoção e divulgação do programa de capacitação; as métricas indicam um bom impacto na capacitação, consciencialização e comportamentos dos cidadãos e ou trabalhadores (exemplificando, se em determinada organização, que aplicou o programa de capacitação aos seus trabalhadores, ocorrer uma diminuição dos incidentes de cibersegurança, pode significar que os conteúdos do programa se aproximaram das necessidades previamente identificadas, isto é, que a percentagem de utilizadores sensibilizados para a temática da cibersegurança aumentou e a percentagem de utilizadores com responsabilidades em cibersegurança formados adequadamente também aumentou); o reconhecimento através da atribuição de prémios, pela partilha de contribuição de cibersegurança; e os decisores, os trabalhadores que desempenham papéis fundamentais na gestão, os trabalhadores envolvidos na coordenação do programa de capacitação em cibersegurança demonstram compromisso com o programa e motivação para promover o mesmo.

5.2. O E-Learning e a cibersegurança

O E-Learning é hoje um método de aprendizagem comumente utilizado e massificado, inclusivamente pela própria academia que tem como base de ensino as aulas presenciais. Estes sistemas são complexos e visam garantir a satisfação do aluno e manter uma boa imagem do processo de aprendizagem. Existem atualmente evidências claras de que as tecnologias educacionais inovadoras, como o E-Learning, oferecem oportunidades sem precedentes para estudantes, professores e outros profissionais que desejem adquirir, desenvolver e manter competências e conhecimentos essenciais (Ali Alowayr and Atta Badi, 2014).

Nos últimos anos o E-Learning, passou por um desenvolvimento admirável. (Latifa Ben Arfa Rabai, 2012). Estes sistemas têm uma enorme variedade de utilizadores e de recursos e a partilha de informações, a colaboração e a interconetividade são os elementos fundamentais de qualquer sistema de E-Learning. Contudo, os dados devem ser protegidos de forma a manter a confidencialidade, a integridade e a disponibilidade, sendo necessário garantir a segurança das informações para, por exemplo, proteger o sistema relativamente à manipulação de dados e à autenticação de falsos utilizadores.

O *Learning Management System* (LMS) é a plataforma de E-Learning, isto é, o ambiente onde o curso ou módulo de formação *online* é desenvolvido e onde os recursos que suportam a aprendizagem estão alojados. É nesta plataforma que é efetuado o planeamento e a implementação dos cursos (alojamento, distribuição e gestão de conteúdo), bem como a avaliação dos participantes. Como exemplos de plataformas de E-Learning temos o edX, WebCT, Moodle e Blackboard.

As mais recentes plataformas de E-Learning modificaram a ideia sobre a educação à distância, aumentando as possibilidades de ensino/formação para quem considera o E-Learning uma opção. As empresas aproveitaram desde cedo os benefícios desta solução, estimulando uma forma mais

eficiente, abrangente e didática de promover a formação, capacitação e consciencialização dos seus trabalhadores.

De acordo com o estudo da E-Learning Market Trends & Forecast 2016 Report[47] (DOCEBO, 2016), o E-Learning poderá ser bastante útil para as organizações, isto porque a estratégia de usar a capacitação, formação e consciencialização *online* permite atualizar os conhecimentos dos trabalhadores sobre as últimas tendências nas suas respetivas áreas, sobre áreas adjacentes, sobre conceitos e políticas gerais ou específicas da organização, entre outras.

Utilizar o E-Learning nas organizações pode ser uma excelente solução para capacitar trabalhadores, investindo no desenvolvimento profissional, num curto espaço de tempo e com ótimos resultados. De uma forma genérica, foram identificadas algumas vantagens em utilizar uma plataforma de E-Learning no programa de capacitação de cidadãos em cibersegurança que nos propomos desenvolver. Nomeadamente a Acessibilidade e Conveniência - os materiais de E-Learning podem estar acessíveis permanentemente, permitindo aos cidadãos e trabalhadores a aprendizagem dos temas ao seu ritmo e da forma que lhes for mais conveniente, independentemente do local onde estão a trabalhar; a Agilidade - permite rapidamente comunicar novas políticas/regras ou ideias, difundir novos conceitos e capacitar ou reforçar capacitação; a Melhoria da Pedagogia – utilizando por exemplo, técnicas de *gamification*[48] que aumenta o envolvimento dos participantes e incrementa a retenção da informação, o uso de materiais de estudo personalizados e formatos interativos, que permitem relacionar competências com o atingir dos objetivos pretendidos pelas organizações; o Aumento da colaboração e do alcance – estas ferramentas permitem aceder instantaneamente aos cidadãos e colaboradores dispersos por diferentes localizações, departamentos e, equipas; Mais Sustentável e com Eficácia de Custos – na era da sustentabilidade, é importante que o Estado e as organizações consigam diminuir os custos relativamente aos sistemas de capacitação convencionais, uma vez que a maior fatia financeira tem a ver com as deslocações de colaboradores e formadores, o aluguer de infraestruturas, o custo-hora do formador e não menos importante a impressão de documentação, por outro lado um programa de E-Learning é mais sustentável, pois não contempla custos de deslocação, de aluguer de salas, de logística associada e os custo com os formadores e com o desenvolvimento dos programas é feito uma única vez; Adequado às novas gerações, comumente referenciadas com *Millennials,* hoje em dia os melhores colaboradores (e consequentemente os mais disputados) escolhem as organizações não apenas pela vertente financeira, mas também pela aprendizagem contínua e através da formação em E-Learning, o conhecimento está à disposição dos colaboradores quando estes quiserem e pode permitir-lhes aceder a temas que lhes interessam, mas que no formato convencional não seriam prioritários, por não terem aplicação imediata no seu dia-a-dia, neste sentido estes colaboradores ficam mais valorizados por um lado e por outro lado pode contribuir para um fator de diferenciação na retenção dos colaboradores, uma vez que as empresas que proporcionam aos seus colaboradores E-Learning de qualidade e com temas valiosos obtêm comprometimento e lealdade

[47] www.docebo.com/2016/06/16/elearning-trends-market-2016 (DOCEBO, 2016)

[48] Gamification - Os colaboradores podem ser envolvidos numa espécie de concurso, criando uma competitividade saudável e promotora do entusiasmo pela aprendizagem

dos mesmo; Gestão da Atividade e Medição do ROI[49] **-** usando um sistema de gestão da formação, não será difícil avaliar os progressos de aprendizagem dos formandos e obter relatórios sobre a sua evolução, neste sentido, a empresa pode criar objetivos gerais de formação/competências, dando aos formandos a liberdade de gestão do processo para os atingir, podendo a cada momento, verificar o comprometimento de cada colaborador com o seu próprio desenvolvimento e aferir em tempo real a eficácia de determinado programa de capacitação/formação.

Após a decisão do sistema de formação ser o E-Learning, é necessário escolher cuidadosamente a plataforma. Também neste caso existem algumas considerações que devem ser tomadas em linha de conta, nomeadamente a possibilidade de utilização de vídeos – pois uma das principais ferramentas de E-Learning é, sem dúvida, o vídeo e este é indispensável porque transmite o conteúdo de forma didática e dinâmica; Funcionalidades que permitam a gestão do conteúdo e a parametrização dos elementos visuais, informações bem estruturadas com cores apropriadas e elementos estrategicamente disponibilizados influenciam bastante na experiência das pessoas e, consequentemente, o sucesso do curso. Neste sentido, também a possibilidade de personalizar o ambiente de estudo deve ser uma opção; A existência de um espaço de Fórum para fomentar o debate sobre temas específicos, esclarecimento de dúvidas, dentre outros, é uma opção altamente enriquecedora da formação on-line, pois permite uma maior aproximação entre os colaboradores e incentiva o troca de informações e de conteúdo relevantes melhorando o ambiente da formação; A emissão de Certificado Digital aos participantes é uma ferramenta indispensável pois permite parametrizar os requisitos para a obtenção do documento, como seja a frequência, ou o desempenho nas avaliações, por exemplo; A Segurança da plataforma é, na nossa opinião, um dos aspetos fundamentais, uma vez que não é suficiente que os conteúdos sejam de qualidade, mas também que tratem da preservação e previna o acesso ilegítimo dos materiais, i.e a plataforma deve funcionar com protocolos seguros e ter o conteúdo cifrado; e por fim permitir uma boa Gestão on-line, desta forma, além dos requisitos técnicos anteriormente explanados, é necessário que a plataforma permita simultaneamente a manutenção dos conteúdos e a análise estratégica dos rotinas de formação dos formandos, permitindo, identificar pontos que aumentem a assertividade da formação e a gerir todas as informações importantes de acompanhamento do desempenho dos formandos.

Escolher a plataforma de E-Learning certa é fundamental para garantir o sucesso da formação aos colaboradores das organizações e aos cidadãos em geral. Neste sentido e porque desejamos que este projeto de capacitação em cibersegurança esteja acessível a todo e qualquer cidadão nacional, na decisão vamos tomar em linha de conta todos os tópicos abordados anteriormente e também as ferramentas necessárias para transmitir os conteúdos de forma atrativa e que proporcione dinamismo no processo de aprendizagem dos cidadãos.

[49] ROI - Return on investment - Retorno sobre o investimento ou taxa de retorno do investimento

5.3. Os MOOC e a Cibersegurança

A tecnologia digital tem vindo a sofrer uma acelerada expansão e dispersão, o que tornou os Massive Open *Online* Course (MOOC) numa modalidade de distribuição massiva do conhecimento, transformando a formação e a educação numa lógica mais aberta, equitativa e flexível.

Os MOOC são cursos abertos disponíveis por meio de ambientes virtuais de aprendizagem, gratuitos e permitem a inscrição de um grande número de participantes, são um progresso relativamente recente na área do E-Learning e dos ideais de educação aberta sugerido pelos REA[50] - Recursos Educacionais Abertos. Potencialmente, os MOOC poderão transformar os atuais cursos de E-Learning em algo mais escalável, sustentável e rentável.

Na vertente organizacional, os MOOC poderão representar uma relevante ajuda nos processos de formação e de requalificação de ativos, proporcionando condições para a criação de redes e de comunidades virtuais que promovam a interação e a colaboração entre os participantes, através da troca, da partilha e da redistribuição de conhecimentos. Podendo ser utilizados como promotores da constituição de comunidades virtuais de aprendizagem, os MOOC favorecem a globalização do conhecimento contribuindo para a inclusão social, à escala mundial, mediante a aproximação do conhecimento à sociedade.

A nossa pesquisa levou-nos ao encontro de Cormier que defende que "*Um MOOC é um curso, é aberto, participativo, distribuído e que suporta a aprendizagem ao longo da vida*" (Cormier, 2010). O autor refere que o MOOC não é uma escola e não é só um curso *online*, sendo sim um evento no qual um número massivo de pessoas, que se preocupam com determinado tema, se reúne e discutem sobre o mesmo de forma estruturada, vindo daí a denominação de curso.

Resumindo, os MOOCs são cursos *online* desenhados e criados para uma grande quantidade de participantes, permitem que qualquer pessoa possa aceder em qualquer lugar, estando subjacente a necessidade de ligação à internet, são gratuitos e abertos a todos sem restrições.

As quatro dimensões centrais do conceito de MOOC estão expostas na tabela seguinte:

Tabela 1- Dimensões de um MOOC (adaptado de Jansen & Schuwer, 2015)

Acrónimo	Significado	Definição da dimensão	Critérios decisivos de um MOOC
M	**Massive**	Curso *online* concebido para um número infinito de participantes	O número de participantes é maior que aquele que pode ser ensinado numa situação "normal" em sala de, A estrutura massiva e o modelo pedagógico do curso é tal que os esforços de todos os serviços não aumentam em função do número de participantes

[50] REA - Recursos educacionais abertos é movimento de uma comunidade internacional impulsionado pela Internet que tem como objetivo promover o acesso, uso e reuso de conteúdos educacionais. Está baseado na ideia de bens comuns

O	**Open**	Qualquer pessoa pode aceder ao curso, independentemente do local que se encontre, desde que tenha conexão à internet	Os cursos estão acessíveis a ´praticamente todas as pessoas sem impor limitações, Os conteúdos estão sempre acessíveis, O curso pode ser acedido em qualquer lugar, pressupondo a existência de ligação à internet
		Aberto e livre ao nível do local, ritmo e tempo	A maioria dos MOOC têm uma data fixa de início e fim, não sendo abertos em ritmo ou tempo, Um ritmo pré-definido e /ou datas fixas de início e fim não são considerados critérios explícitos a distinguir entre MOOCs e outros tipos de cursos
		Aberto para todos sem exigir pré-requisitos e/ou qualificações	Não são exigidos pré-requisitos e/ou qualificações/certificações para participar no curso
		O curso pode ser concluído gratuitamente	Os formandos participam por completo no curso sem qualquer tipo de custos
O	***Online***	Curso totalmente *online*	Todas as indicações, referências e conteúdos do curso são disponibilizados *online*
C	**Course**	Unidade de estudo	O tempo total de estudo de um MOOC corresponde, no mínimo a 1 ECTS (e varia normalmente entre 1 e 4 ECTS)
		Contém uma sequência sistemática de atividades de aprendizagem, que inclui: Conteúdos educativos	Os conteúdos educativos podem incluir recursos como vídeo, áudio, texto, jogos (incluindo simulações), social media, animações, entre outros
		Facilidade na interação entre pares (no entanto, a interação com o tutores pode ser limitada)	Oferece possibilidades de interação, através de redes sociais, fóruns, blogues para construir uma comunidade de aprendizagem
		Atividades / tarefas, testes, incluindo *feedback*	Existem mecanismos de *feedback* para os participantes, que podem ser gerados automaticamente (através de questionários, por pares- *feedback* de pares e/ou *feedback* geral dos tutores)
		Opções de reconhecimento/certificação (formal/informal)	São incluídas várias formas de reconhecimento dos conhecimentos e/ou competências alcançadas por parte dos participantes que finalizam o curso (reconhecimentos informais- badges, e outros mais formais, adquiridos mediante pagamento- certificados de participação, de classificação, entre outros)

		Um guia/plano de estudos	O guia/plano de estudos inclui as instruções e indicações de como aprender através dos materiais e recursos do curso

Consideramos que no caso do nosso programa de capacitação de cidadãos em cibersegurança, o 'M' de Massivo é o mais relevante, pois refere-se à capacidade dos MOOC suportarem um número ilimitado (com centenas ou mesmo milhares) de participantes, não impondo número máximo de inscrições.

A realização em grande escala é uma das características que diferencia os MOOC de outros cursos *online* abertos. O termo 'massivo' não tem associado um número específico de participantes, no entanto, a capacidade massiva dos MOOC é fruto do desenvolvimento da pedagogia *online* de ensino à distância e das TIC, através dos avanços de infraestruturas e de software de armazenamento, indexação e acesso a grandes quantidades de conteúdos digitais, como sendo do YouTube, do Google Books, de bibliotecas digitais, de soluções baseadas na Cloud entre outras; da identificação e posterior registo seguro de grande número de potenciais participantes e de Software e serviços robustos, confiáveis e seguros para acesso em simultâneo de um elevado número de utilizadores para as mesmas páginas web.

5.3.1. A certificação dos MOOC

Nos cursos MOOC poderemos ter diversos tipos de certificação ou mesmo a Inexistência de certificação, isto é, após a conclusão do curso, não existe hipótese de atribuir certificado aos participantes; Certificados digitais (*badges*): a atribuição de *badges* é um *standard* visual que divulga na rede as competências do participante; Certificado de participação: só têm direito a este certificado os participantes que tenham participado em grande parte das atividades obrigatórias previstas no curso (uma média de 75%), sendo o certificado gratuito e passível de ser descarregado eletronicamente; Certificado de Superação: em que os participantes que tenham realizado todas as atividades obrigatórias incluídas no curso e superado todas as avaliações parciais e a prova final obtém um Certificado de Superação, que pode ser descarregado eletronicamente após a conclusão do curso com uma taxa associada, cujo valor varia consoante o curso e duração do mesmo; e por fim Certificado de Acreditação: em que os cursos atribuem créditos mediante o pagamento de uma taxa, que permite aos participantes o acesso ao curso, à supervisão, à comunicação direta com tutores e exames *online*, e ainda uma prova final com um exame presencial que permita comprovar a identidade do formando que frequentou o curso e realizou a prova final. A emissão deste certificado tem uma taxa associada que varia em função do curso, da duração e da localização do formando.

No caso do nosso programa de capacitação de cidadãos em cibersegurança, sugere-se a certificação digital através de um *badge* ao participante e à organização. Ao participante será atribuído um *badge* digital desde que obtenha uma pontuação superior a 85% de respostas corretas – *badge* de cibercidadão. No caso das organizações este selo certificaria as organizações que tivessem mais de 75% de cibercidadãos, isto é mais de 75% de trabalhadores da organização certificados em cibersegurança pelo programa de capacitação de cidadãos em cibersegurança.

Construção de um MOOC

O desenho de um MOOC deve incluir o mesmo conjunto de elementos curriculares que qualquer outro curso de formação inclui, nesse sentido deveremos considerar os objetivos, os conteúdos, os meios e a avaliação.

No desenvolvimento de um curso, as responsabilidades a ter em conta (Costa, Santos , Silva , & Viana , 2015) são as elencadas de seguida:

- Descrever de forma genérica o curso (apresentar o curso através de uma síntese contextualizadora e introduzir aos tópicos a abordar, por exemplo através dum *teaser* (vídeo) promocional da visão global e do enquadramento do curso);
- Definir o público alvo/audiência a que se destina o curso (características gerais do perfil ou perfis dos participantes);
- Definir os pré-requisitos, se existirem (necessidade de preparação prévia ou conhecimentos específicos para participar no curso);
- Definir os objetivos gerais de aprendizagem (pode ser considerada a aquisição de conhecimentos, o desenvolvimento de capacidades e as atitudes por parte dos participantes);
- Listar e organizar os tópicos que irão ser trabalhados no curso (tema e estrutura interna dos tópicos que serão desenvolvidos no curso). Normalmente a estrutura do MOOC assenta em conteúdos estruturados em tópicos numa base semanal e para cada um dos tópicos os objetivos de aprendizagem devem ser especificados, explicando aos formandos os resultados de aprendizagem esperados e o tipo de atividades que servirão para avaliar as competências adquiridas. Os tipos de conteúdos de aprendizagem a utilizar em cada um dos tópicos também deve ser definido, e poderão ser vídeos - vídeo simples, vídeo com voz *off*, vídeo com slides e/ou quadro interativo e/ou articulação destes com outros materiais, ou poderão ser textos, imagens, hiperligações, entre outros. É importante que os vídeos expositivos sejam curtos e objetivos (5-10 minutos cada);
- Explicitar as estratégias e os modos de organização do trabalho selecionado;
- Explicitar as modalidades de interação, de comunicação e de colaboração (fóruns de discussão/grupos de trabalho, acompanhamento e esclarecimento de dúvidas, atividades síncronas/assíncronas);
- Explicitar os objetivos as modalidades de avaliação escolhidas (avaliação de diagnóstico, avaliação formativa, avaliação sumativa, autoavaliação, avaliação por pares, quando se atribui certificação e as respetivas condições);
- Definir a calendarização (datas de início e fim)
- e a Definição da Equipa dinamizadora (membros que compõe a equipa responsável pelo curso - programador, técnicos, outros profissionais).

A Universidade do Porto (2015) para avalizar a coerência pedagógica desenvolveu um documento onde descreve o que deve ser o Modelo pedagógico recomendado para MOOCs, compilando a informação na sugestão inserida na tabela seguinte

Tabela 2- Exemplo de estrutura e organização de cursos MOOC **(Porto, 2015)**

APRESENTAÇÃO DO CURSO (informação generalista disponível ao público) Vídeo de divulgação/apresentação Data do curso (início/fim) Data para inscrição (início/fim) Breve descrição do curso (+/- 150 caracteres) Descritivo do curso Programa Objetivos de aprendizagem Formato Duração Certificação Pré-requisitos	1ª SEMANA	**INTRODUÇÃO**		
		Vídeo de boas vindas com apresentação dos professores, estrutura do curso e objectivos		
		MÓDULO 1		
		M1 – Tópico N		
		Introdução: Objectivos de aprendizagem	**Conteúdos:** Vídeos Textos	**Atividades/ Avaliação:** Fóruns Testes
	2ª SEMANA	**MÓDULO 2**		
		M2 – Tópico N		
		Introdução: Objectivos de aprendizagem	**Conteúdos:** Vídeos Textos	**Atividades/ Avaliação:** Fóruns Testes
		M2 – Tópico N		
		Introdução: Objectivos de aprendizagem	**Conteúdos:** Vídeos Textos	**Atividades/ Avaliação:** Fóruns Testes
	3ª SEMANA	**MÓDULO 3**		
		M3 – Tópico N		
		Introdução: Objectivos de aprendizagem	**Conteúdos:** Vídeos Textos	**Atividades/ Avaliação:** Fóruns Testes

Um dos pontos que salientamos como de especial relevância é o facto do programa de capacitação de cidadãos que nos propomos desenvolver ter de ter em consideração a estratégia institucional da organização, nomeadamente, a missão, os objetivos e as preocupações explícitas a curto e longo prazo, a gestão de projetos, o programa curricular, a equipa de projeto, os recursos pedagógicos, as características dos participantes, a plataformas *online* e os recursos financeiros.

Para garantir a qualidade pedagógica e gráfica, bem como o rigor científico do curso de cibersegurança para cidadãos, é necessário selecionar recursos humanos (equipa multidisciplinar/profissionais técnicos) com competências reconhecidas, que incorporem no curso as ferramentas e os recursos mais adequados.

Pelo facto de se tratar de uma proposta de um programa de capacitação de cidadãos, cujas dimensões *open* e *online* são uma premissa, o curso deve conter componentes e recursos disponibilizados *online*, confirmando a qualidade e destacando-se pelos aspetos inovadores, pedagógicos e tecnológicos, que possa trazer.

5.4. Desenvolver o Programa de Capacitação em Cibersegurança para Cidadãos

Ao longo desta dissertação já foi referido, algumas vezes, que uma organização é tão mais segura, do ponto de vista da segurança dos sistemas de informação e da informação propriamente dita, quanto mais consciente dos riscos estiveram os trabalhadores da mesma. Os complexos desafios da segurança do ciberespaço surgem a todo o momento, pois a maioria dos trabalhadores (se não todos) estão *online* e os seus dispositivos móveis no seu local de trabalho também, a indústria das Tecnologias de Informação disponibiliza software com milhões de linhas de código e com vulnerabilidades embutidas, e o resto da organização abre e-mails, independentemente de saber ou não o remetente.

Tanto nas organizações maiores como nas mais pequenas, os incidentes de cibersegurança têm-se mostrado ao longo dos últimos anos cada vez mais frequentes e complexos. Sensibilizar cidadãos e formar trabalhadores sobre os riscos e sobre como fazer o seu trabalho de forma segura é a única forma verdadeira de mitigar o impacto e reduzir os danos decorrentes de incidentes desta natureza.

Os incidentes de cibersegurança não discriminam organizações nem cidadãos, ocorrendo em sistemas de informação vulneráveis, independentemente de pertencerem a uma grande organização, a uma pequena empresa ou pertencer a um utilizador comum. A cibersegurança deve assim ser uma responsabilidade partilhada e todos os cidadãos e trabalhadores devem ter um papel a desempenhar. O Programa de Capacitação em Cibersegurança que nos propomos desenvolver e implementar fornece sugestões de recursos para todos os segmentos da sociedade.

Neste sentido, apresentamos uma tabela, a que chamamos a tabela das Dimensões em cibersegurança, que mostra por segmentos da sociedade (função profissional), as necessidades e o nível de competências em cibersegurança a adquirir (A – Alto, M- Médio, B- Baixo), subdividas por vetores de ação.

Tabela 3- Tabela das Dimensões em Cibersegurança

Dimensões de cibersegurança

	Organizativa /Gestão	Económica	Legal	Técnica	Comportamental
Alta direção/ Administração	A	M	M	B	A
Direção intermédia	M	A	M	B	A
Gestor técnico (TIC)	B	B	B	A	A
Gestor Funcional (área financeira, recursos humanos, compras, logística, …)	B	M	A	M	A
Funcionário / cidadão			B	B	M

Legenda: A – Alto, M- Médio, B- Baixo

A Cibersegurança nas organizações é uma área de atuação multidisciplinar e com impacto direto na governação organizacional. Como tal, tópicos como a liderança estratégica e o pensamento crítico no desenvolvimento de processos e decisão na utilização da tecnologia, vertidos nas estratégias de cibersegurança são essenciais. Também a existência de planos de segurança e políticas organizacionais; de matrizes de formação e avaliação, de gestão de risco, de gestão de incidentes e planos de continuidade de negócio devem ser considerados, garantindo alinhamento de pessoas, processos e tecnologias com a missão e objetivos da organização. Consideramos assim que os fatores referidos anteriormente são vetores fundamentais na dimensão organizativa e de gestão da cibersegurança pelos Administradores das organizações, sendo também vetores importantes para os dirigentes que desempenham funções de direção intermédia e para gestores técnicos e gestores funcionais.

Os novos mercados impõem uma nova perspetiva e criam novos desafios. As parcerias público-privadas (PPP), a colaboração e cooperação no desenvolvimento comum da Cibersegurança são algumas das dimensões económicas no seio da cibersegurança que devem ter especial capacitação pela direção intermédia. As responsabilidades associadas à administração e aos gestores funcionais também deve ter uma relevância significativa e, por fim, no caso dos gestores técnicos, a capacitação económica tem uma relevância menor.

Do ponto de vista dos desafios legais, o enquadramento legal da Cibersegurança, os direitos fundamentais e direitos humanos, a privacidade e proteção de dados pessoais, são alguns dos mais prementes, a par da proteção da propriedade intelectual e da importância do mercado único digital. Outros desafios relevantes são ainda o comércio eletrónico na União Europeia, a promoção da ação judiciária, a cooperação internacional judiciária (no conceito alargado de segurança e Cibersegurança), as vontades versus os compromissos dos Estados no palco internacional, o Direito Internacional Público enquanto instrumento regulador e de aplicação formal em espaço não regulado e tutelado.

Todos os desafios acima referidos são alguns dos que devem ser considerados na capacitação de todos os níveis funcionais, com níveis de profundidade distintos.

A perspetiva prática de algumas tipologias comuns de incidentes de segurança informática, as metodologias de um ciberataque (a sua infraestrutra ofensiva) e as suas fases, a capacitação nacional através dos Modelos de Maturidade de Reação, Deteção e Prevenção de ciberincidentes, de forma a garantir uma aproximação coerente e compreensiva da maturidade organizacional para a cibersegurança, são os vetores fundamentais, mas não exclusivos, com níveis distintos de capacitação dos profissionais que trabalham em todas as áreas funcionais da organização.

O fator humano, nomeadamente os comportamentos, são fundamentais e transversais, devendo ser tomados em linha de conta na cibersegurança. Se determinados comportamentos não fizerem parte da cultura da organização e se não foram tidos como primordiais na prevenção dos incidentes internos ou externos, então não existem Sistemas de Informação suficientemente robustos que protejam o utilizador das potenciais ameaças. As ameaças a que nos referimos dizem respeito à exploração do comportamento humano, como seja a desorganização, o desleixo, o comentar assuntos profissionais ou mesmo a ignorância. Educar, formar, capacitar, consciencializar e sensibilizar os colaboradores e os cidadãos para os comportamentos adequados a uma cultura organizacional de cibersegurança é a base para fortalecer as organizações.

A consciência da Cibersegurança deve começar no topo da pirâmide da organização. As funções de administração e de direção intermédia necessitam de ter uma noção exata dos riscos, não só para a organização como um todo, mas também como eles próprios podem colocar a organização em risco se não forem cuidadosos. Muitas vezes, os trabalhadores que desempenham funções de gestão são algumas das vítimas dos *hackers*[51], principalmente devido à sua proximidade da informação com um grau de importância significativo, podendo ser um alvo preferencial de um ataque de *ransomware* ou de *phishing*, por exemplo.

Por outro lado, os trabalhadores das áreas técnicas e de gestão funcional têm um papel diferente, mas altamente influente em apoiar, criar e manter uma organização segura. São eles que podem trazer à gestão de topo das organizações informação técnica atualizada sobre os novos desafios e riscos com que as organizações se defrontam.

Por fim, todos na organização necessitam de entender que a segurança da organização depende de todos e de cada um dos funcionários em particular. Basta uma palavra-passe fraca, um email de *phishing* respondido, um computador desbloqueado ou um telefone roubado e desbloqueado, para poder destruir a organização. É por esta razão que se torna necessário garantir que os trabalhadores, e os cidadãos em geral, usufruam de programas de ciber-higiene. Muitos incidentes poderiam ter sido evitados com apenas um pouco mais de consciencialização e formação de cibersegurança. No futuro, somente com o contributo da formação adequada poderemos contribuir para a redução e mitigação dos incidentes.

[51] Pessoa que possui interesse e um bom conhecimento de informática que é capaz de fazer modificações nos sistemas informáticos

Podemos afirmar que todos os segmentos da sociedade (funções profissionais) necessitam de consciencialização, no entanto, no âmbito deste trabalho, o programa de capacitação em cibersegurança que nos propomos desenvolver cinge-se exatamente às competências de cibersegurança que qualquer trabalhador ou cidadão deve possuir, que mais não é do que, a intersecção da dimensão comportamental com o fator humano. Esta intersecção (curso) deve ter um nível de profundidade médio.

A autora deste projeto esteve envolvida na conceção e desenvolvimento de outros cursos de consciencialização para públicos específicos, nomeadamente, nos cursos de E-Learning do Centro de Formação do Instituto Diplomático do Ministério dos Negócios Estrangeiros (MNE). Os cursos a que nos referimos destinam-se à formação dos funcionários dos serviços internos e externos. Estando os serviços e representações do MNE distribuídos geograficamente à escala mundial, a formação à distância assume um relevo particular, pelo que foram fornecidos conteúdos de cibersegurança para posterior conceção do módulo de cibersegurança do Curso de Segurança da Informação – Matérias Classificadas 2017, e ainda uma diversidade relevante de conteúdos para construir vários módulos distintos do Curso de Cibersegurança. O primeiro já se encontra disponível na Plataforma de Formação do MNE (figura 9) e o segundo encontra-se em produção.

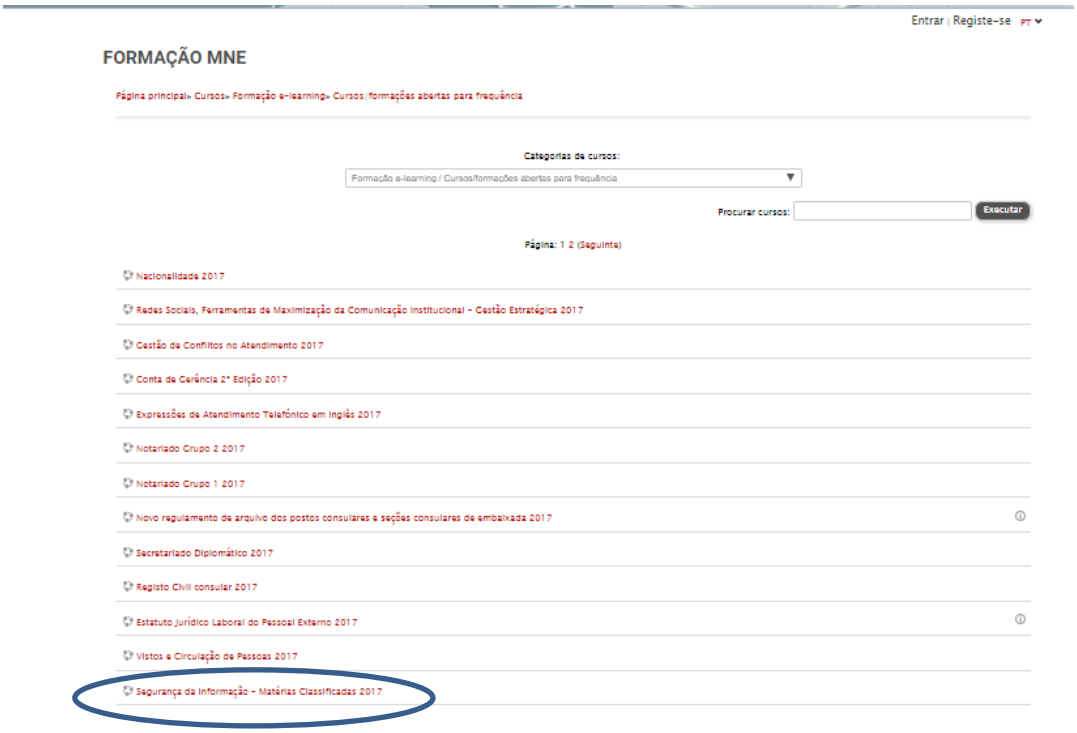

Figura 9 - Catálogo de cursos do MNE, destacando o curso de Segurança da informação – Matérias classificadas 2017

A autora esteve também envolvida na génese do Curso Geral de Cibersegurança que o CNCS disponibiliza presencialmente a todos os quadros intermédios e superiores das estruturas do Estado e da sociedade civil, bem como aos elementos com potencial para o desempenho de funções de gestão de segurança numa vertente tecnológica. Este curso tem uma perspetiva *whole-of-society* e tem como principal objetivo responder à necessidade de existência de uma formação holística e de curta duração

que foque todas as dimensões da cibersegurança - competência organizativa/gestão, económica, legal, técnica e comportamental com níveis de profundidade Médio ou Baixo.

A conceção dos conteúdos, dos módulos, dos cursos de sensibilização presenciais, a públicos e organizações específicos do Estado têm o envolvimento da autora. Estes cursos pretendem também sensibilizar para a adequação dos comportamentos do fator humano aos desafios da utilização do ciberespaço. São cursos de pequena duração (1 a 2 horas) e destinam-se a transmitir competências de cibersegurança da vertente organizativa, económica, legal e comportamental com um nível de profundidade de conteúdos médio e baixo (dependente da competência).

Da experiência adquirida e da necessidade premente de sensibilizar de forma transversal a sociedade, os cidadãos e os trabalhadores em geral (necessidade destacada na tabela 8), propomos a construção de um curso de E-Learning, recorrendo à metodologia MOOC.

Para que este curso chegue ao maior número possível de cidadãos será necessário que o mesmo tenha uma divulgação massiva. Neste sentido, sugere-se que o *link* de acesso ao curso esteja disponível no sítio do GNS e do CNCS, nos sítios das diferentes áreas do Governo e das secretarias gerais respetivas, nas intranets do maior número possível de organismos do Estado e nos sítios dos serviços do Estado com ligação direta ao cidadão. Pretende-se que este programa de capacitação de cidadãos em cibersegurança seja entendido como uma responsabilidade social dos organismos do Estado para com os cidadãos em geral no domínio da cibersegurança.

Este programa de capacitação de cidadãos em cibersegurança, além do curso de E-Learning que nos propomos desenvolver, deve ainda ser complementado com um plano de comunicação que contemple diversificados meios de comunicação, como sendo folhetos informativos e desdobráveis, cartazes e posters, merchandising, vídeos, *posts* nas redes sociais das organizações, do GNS e do CNCS em particular, com mensagens simples, diretas e percetíveis pela generalidade dos cidadãos.

A nossa proposta para o curso de E-Learning de cibersegurança para capacitação de cidadãos e funcionários, na vertente comportamental e com um nível de profundidade médio, enquadra-se na nossa tabela de dimensões em cibersegurança (figura 9) na intersecção do eixo do cidadão com a vertente comportamental (figura 10).

	Organizativa/ de Gestão	Económica	Legal	Técnica	Comportamental
Funcionário / cidadão			B	B	M

Legenda: A – Alto, M- Médio, B- Baixo

Figura 10 – Enquadramento do curso de capacitação de cidadãos em cibersegurança

Para o curso de E-Learning de cibersegurança de cidadãos e funcionários sugere-se o seguinte programa de curso:

Curso de CiberCidadão – Dimensão Comportamental

Nível M (Médio)

Acerca do curso

Título do Curso	Ciber-higiene
Destinatários	Cidadão / sociedade civil
Módulos Facultativos	Navegação sénior Navegação segura (por grupos de risco)
Duração	4 semanas
Esforço	2 a 5 horas por semana
Condições financeiras	Gratuito
Idioma	Português
Certificado	O certificado será atribuído, após conclusão do curso no período de frequência definido e após obtenção de um número de resposta corretas superior a 85% (oitenta e cinco por cento)
Data de conceção	Maio de 2017
Data da última revisão dos conteúdos	
Autores (conteúdo e desenho gráfico)	A definir
Desenvolvimento do curso	A definir
Integração Plataforma	A definir
Propriedade	CNCS

Contexto

O curso propõe desenvolver um currículo inovador sobre os comportamentos digitais e a importância das boas práticas de segurança no ciberespaço na vertente comportamental da segurança da informação, de forma a prevenir incidentes de cibersegurança tanto nos indivíduos como nas organizações. Esta vertente diz respeito à ciber-higiene do indivíduo, que se restringe à instituição e manutenção de rotinas diárias, a rotinas de verificações e aos comportamentos gerais necessários para manter a "saúde" de um cidadão/funcionário de uma organização.

Objetivos:

- Compreender a dimensão humana do risco de cibersegurança;

- Estar consciente relativamente aos riscos introduzidos nos sistemas, nas ferramentas internas e externas das organizações, e em todos os dispositivos como *tablets*, *smartphone, laptops, smartwatch*, entre outros.
- Promover a cibersegurança na vida profissional e privada

Módulos:

- Gestão de palavras passe
- Navegação segura
- Engenharia social
- *Email, Phishing*, & Mensagens
- Redes sociais
- Segurança em viagem nacional/internacional
- Segurança de *smartphones*
- Proteger as redes domésticas
- Proteger o computador pessoal
- Trabalhar remotamente e segurança de redes wi-fi
- Navegação sénior (módulo facultativo)
- Navegação segura (por grupos de risco – módulo facultativo)
- *Firewall* humana

Atividades de aquisição de conhecimentos:

- Visualização de vídeos
- Leitura de documentos
- Visualização de apresentações
- Questionário de avaliação intermédio com relatório de melhoria contínua (fomentar o aprofundamento da aprendizagem e a mudança de comportamento)
- Conteúdo de treinamento interativo

Avaliação:

- Questionário de avaliação final - avaliação final do nível de conhecimentos adquiridos. O certificado será atribuído, após conclusão do curso no período de frequência definido e após obtenção de um número de resposta corretas superior a 85% (oitenta e cinco por cento)

5.5. Avaliação

Em qualquer curso ou módulo os mecanismos formais de avaliação e de comunicação de resposta (*feedback*) são componentes críticos. Os mecanismos de *feedback* devem ser delineados para focar os objetivos principais do curso. Podem ser diversos os mecanismos de avaliação e de

comunicação de resposta ou realimentação, que podem ser utilizados para manter atualizado o curso ou módulo, nomeadamente os formulários de avaliação, a observação independente, os relatórios intermédios de *feedback* ao cidadão, entrevistas, grupos focais, *benchmarking*, ente outros.

Na estratégia de avaliação e de realimentação, os seguintes elementos devem ser analisados: qualidade, âmbito, método de implementação (por exemplo, presencial, E-Learning, misto), nível de dificuldade, facilidade de utilização, duração do curso e dos módulos, pertinência dos conteúdos e sugestões de modificação.

Neste âmbito, também as métricas são essenciais e podem ser usadas para medir a eficácia do curso; fornecer informações à organização relativamente aos dados de conformidade; e fornecer um indicador importante para demonstrar o progresso e identificar áreas para melhoria.

Por outro lado, é necessário garantir que o programa de capacitação de cidadãos em cibersegurança, evolua com o emergir de novas tecnologias e novos problemas de cibersegurança resultantes da transformação digital. A sensibilização e a formação terão de andar a par com as novas competências e capacidades que vão sendo necessárias para responder às mudanças de arquitetura e de tecnologia. Outras questões emergentes também terão impacto na sensibilização e na formação sobre as últimas ameaças, vulnerabilidades e medidas a adotar. Novos enquadramentos jurídicos, também poderão afetar as políticas das organizações e por sua vez, impactar no desenvolvimento/atualização de informação a transmitir no programa de capacitação em cibersegurança.

Nas organizações, os decisores, os CIOs, os CISOs e os trabalhadores dos departamentos TIC devem ser os principais defensores dos programas de capacitação em cibersegurança para funcionários, demonstrando comprometimento e apoio.

No caso específico do programa de capacitação de cidadãos em cibersegurança propõe-se que seja efetuada uma avaliação interna periódica (por exemplo, numa base anual), tendo como entrada os dados do RASI, as principais tendências de cibersegurança, a evolução estatística dos incidentes e das ameaças, bem como os relatórios da ENISA sobre lições aprendidas, de forma a poderem ser tomados em consideração nas atualizações dos conteúdos do curso de cibercidadão e/ou no desenvolvimento de novos módulos ou cursos.

Também o *feedback* dos utilizadores e das organizações, comunicados através dos formulários de avaliação, podem-se revelar um precioso contributo, relativamente às métricas a definir no início do curso, que deverão contemplaram entre outros, a qualidade, o âmbito, o nível de dificuldade, a facilidade de utilização, a duração do curso e dos módulos, a pertinência dos conteúdos e sugestões.

6. Conclusão e trabalho futuro

6.1. Conclusão

Os rápidos avanços nas TIC provocam na sociedade contemporânea uma significativa alteração na vida diária. Indivíduos, organizações e Estado, necessitam da Internet e das TIC para a realização das suas tarefas, significando que, genericamente, a sociedade e os indivíduos estão cada vez mais dependentes da tecnologia. Neste sentido, os sistemas de informação são fundamentais para o sucesso da Sociedade de Informação - uma sociedade globalizada, onde predomina a partilha e o simples e fácil acesso à informação.

O constante desenvolvimento de novas ameaças; o aumento de ataques na Internet; o roubo de identidade ou o crime de extorsão, exigem que o cidadão esteja cada vez mais consciente da importância da proteção da sua informação e seja experiente e atento nessa proteção. Sabe-se hoje, que a melhor forma de obter uma melhoria significativa da segurança da informação, é através do aumento da consciência e do adequado comportamento dos indivíduos na utilização dos sistemas de informação. A consciencialização é então o ponto de partida para o desenvolvimento de um programa de capacitação de cidadãos em cibersegurança, bem-sucedido.

São significativos e com uma expressão geográfica bastante considerável, os programas de capacitação de cidadãos existentes. Cada programa analisado, do qual foi efetuada uma revisão de literatura, revelou especificidades próprias do país de origem. Estes contribuíram e foram fonte de inspiração para o programa de capacitação objeto desta dissertação. Para uma adequação mais ajustada á realidade nacional foram ainda analisados com maior minucia os projetos nacionais, tendo como objetivo a não sobreposição de público alvo e de abordagem.

Também os dados do RASI foram objeto de análise, tendo-se concluído que Portugal registou um crescimento do *ransomware* e uma estabilização do uso de moedas virtuais. Sugere este relatório, um maior investimento na sensibilização, nomeadamente nas matérias que impactam no crime informático.

Uma carreira em cibersegurança requer competências relevantes e muitas vezes específicas. No entanto, esta especificidade ainda não se encontra refletida num quadro identificativo das competências ditas relevantes, levando a que se possa encontrar no mercado uma variedade imensa de cursos de formação e de ensino, tipicamente conotados como cursos de requalificação ou reconversão. Escolher o curso/formação é um verdadeiro desafio para quem procura qualificar-se, preparar-se para entrar ou desenvolver uma carreira em cibersegurança escolher o curso/formação.

Na cibersegurança, como noutras áreas, a educação (preparar alguém para o futuro), a formação (ensinar competências) e a capacitação (focar a atenção de um indivíduo num problema/ questões, onde é necessária perceção e adequação do seu comportamento) complementam-se muito confortavelmente, uma vez que a progressão numa função deve ser participada por um envolvimento prudente em ambas as atividades.

Relativamente à capacitação em cibersegurança, esta deve combinar atividades de promoção de segurança, estabelecer responsabilidades e comunicar aos funcionários as últimas notícias e novidades de cibersegurança. Estes programas devem disseminar continuamente, e através de vários formatos, a mensagem de cibersegurança pelos indivíduos utilizando uma multiplicidade de ferramentas, meios de comunicação e divulgação, e desenvolvimento de métricas.

É imperativo que os Estados respondam eficazmente aos desafios que lhes são colocados, pela evolução e pela dependência das sociedades atuais relativamente à informação e pela necessidade de garantia da segurança e da disponibilidade dos serviços críticos que alicerçam estas mesmas sociedades e informações, quase sempre suportadas, de forma direta ou indireta, em infraestruturas e processos tecnológicos.

Os Estados e principalmente as organizações têm um papel fundamental no desenvolvimento das sociedades e na promoção da inovação tecnológica, tomando como premissa a necessidade que os cidadãos têm de competências e de sensibilização para que possam acompanhar a evolução da tecnologia. O sinal de reconhecimento político, de que a cibersegurança é hoje estrategicamente relevante, as opções estratégicas enunciadas pelo Presidente da Comissão Europeia, Jean-Claude Juncker e a referência à falta de consciencialização e conhecimento dos cidadãos para as matérias de cibersegurança, reforçam a confiança e o investimento de que a criação de um programa de capacitação em cibersegurança, terá o acolhimento e a implementação desejada junto dos cidadãos.

Um programa de capacitação em cibersegurança não é mais do que um programa de ciber-higiene que contribuirá, entre outros, para a redução do número de incidentes de cibersegurança que ocorrem por falta de consciencialização, dos cidadãos, para estes temas. Neste sentido, uma forma aliciante de informar os cidadãos e os trabalhadores sobre as atividades maliciosas que ocorrem no ciberespaço e que visam as organizações onde os mesmos trabalham, é convidá-los a participar num programa de capacitação em cibersegurança.

O E-Learning é um método de aprendizagem comumente utilizado e massificado. Estes sistemas são complexos e visam garantir a satisfação do aluno e manter uma boa imagem do processo de aprendizagem. Atualmente, existem evidências claras de que as tecnologias educacionais inovadoras, como o E-Learning, oferecem oportunidades sem precedentes para estudantes, professores e outros profissionais que desejem adquirir, desenvolver e manter competências e conhecimentos essenciais. Por outro lado, as mais recentes plataformas de E-Learning modificaram a ideia sobre a educação à distância, aumentando as possibilidades de ensino/formação para quem considera o E-Learning uma opção. Também, as empresas aproveitaram desde cedo os benefícios desta solução, estimulando a formação, capacitação e consciencialização dos seus trabalhadores.

A tecnologia digital tem sofrido uma acelerada expansão e dispersão, o que tornou os MOOC numa modalidade de distribuição massiva do conhecimento, transformando a formação e a educação numa lógica mais aberta, equitativa e flexível. Desta forma, os MOOCs são cursos *online* desenhados e criados para uma grande quantidade de participantes, que permitem que qualquer pessoa possa aceder em qualquer lugar, estando subjacente a necessidade de ligação à internet, são gratuitos e abertos a todos sem restrições.

Os incidentes de cibersegurança não discriminam organizações nem cidadãos, ocorrendo em sistemas de informação vulneráveis, independentemente de pertencerem a uma grande organização, a uma pequena empresa ou pertencer a um utilizador comum. A cibersegurança deve assim ser uma responsabilidade partilhada e todos os cidadãos e trabalhadores devem ter um papel a desempenhar. O Programa de Capacitação em Cibersegurança que nos propomos concretizar com base nos princípios que aqui desenvolvemos, bem como a sua implementação, fornecem sugestões de recursos para todos os segmentos da sociedade. Neste sentido, foi apresentada uma tabela das Competências em Cibersegurança, que mostra por segmentos da sociedade (função profissional), as necessidades e o nível de competências em cibersegurança a adquirir.

O fator humano, nomeadamente os comportamentos, são fundamentais e transversais, devendo ser tomados em linha de conta na cibersegurança. Se determinados comportamentos não fizerem parte da cultura da organização e se não foram tidos como primordiais na prevenção dos incidentes internos ou externos, então não existem Sistemas de Informação suficientemente robustos que protejam o utilizador das potenciais ameaças. Educar, formar, capacitar, consciencializar e sensibilizar os colaboradores e os cidadãos para os comportamentos adequados a para uma cultura organizacional de cibersegurança é a base para fortalecer as organizações.

Todos os segmentos da sociedade (funções profissionais) necessitam de consciencialização, no entanto, o programa de capacitação em cibersegurança que nos propomos desenvolver cinge-se às competências de cibersegurança que qualquer trabalhador ou cidadão deve possuir.

Foi proposta, nesta dissertação o desenvolvimento de um curso de E-Learning, recorrendo à metodologia MOOC, que fomente a consciencialização, de forma transversal, da sociedade, dos cidadãos e dos trabalhadores em geral (necessidade destacada na tabela 8). Para que este curso chegue ao maior número possível de cidadãos, será necessário que o mesmo tenha uma divulgação massiva nos vários sítios do Governo, nas intranets do maior número possível de organismos do Estado e nos sítios dos serviços do Estado com ligação direta ao cidadão.

Este programa de capacitação de cidadãos em cibersegurança, deve ser acompanhado de um plano de comunicação que contemple diversificados meios, como sendo folhetos informativos e desdobráveis, cartazes e posters, *merchandising*, vídeos, *posts* nas redes sociais das organizações, do GNS e do CNCS em particular, com mensagens simples, diretas e percetíveis pela generalidade dos cidadãos.

Para a manutenção e constante atualização dos conteúdos deste programa de capacitação de cidadãos em cibersegurança propõe-se que seja efetuada uma avaliação interna anual, tendo como entrada os dados do RASI, as principais tendências de cibersegurança, a evolução estatística dos incidentes e das ameaças, os relatórios da ENISA sobre lições aprendidas e o *feedback* dos utilizadores e das organizações, comunicados através dos formulários de avaliação do curso.

6.2. Trabalho futuro

Durante a fase de desenvolvimento desta dissertação e da experiência profissional da autora, foi identificada a necessidade de um maior investimento, por parte das organizações e da Administração Pública, em Gestão de *Personware.*

Personware, não é mais do que, os recursos humanos duma organização que permitem o adequado funcionamento do *hardware* e do *software* – os trabalhadores com funções nas áreas de TI.

O mundo atual está repleto de desafios tecnológicos, que provocam uma procura de recursos humanos com competências e capacidades específicas. Por outro lado, as organizações têm nos seus quadros indivíduos que também ambicionam adequar o seu perfil às necessidades do mercado. No processo de crescimento do trabalhador, no seio de uma organização, está inerente o reconhecimento das competências do mesmo, o potencial de aprendizagem, os comportamentos e as necessidades de formação, bem como a antecipação dos requisitos da organização. Por outro lado, na nossa opinião, uma organização que promove o desenvolvimento profissional dos seus trabalhadores, através de um plano de carreira adequado e ajustado que inclua formação profissional, está também a contribuir para a realização dos seus objetivos organizacionais.

Nesse sentido, as organizações devem desenvolver um plano de carreira por trabalhador que contemple, entre outros, a descrição das responsabilidades para o exercício da função, comumente definido como *job description* e a avaliação do trabalhador na função que exerce.

A gestão do *Personware* inicia-se sempre no trabalhador e como ele se enquadra na organização. *Personware*, ao contrário do *software* e do *hardware*, é um mecanismo de autoavaliação, que deve contemplar a descrição da função desenvolvida pelo trabalhador, a posição onde se enquadra na organização, as suas responsabilidades, as tarefas que desenvolve, as competências e a educação ou formação necessárias para o exercício ou evolução das suas funções.

Propõe-se como elemento de estudo futuro, a investigação e posterior implementação de um modelo de Gestão de *Personware* em Cibersegurança, que deve partir de um quadro identificativo das competências relevantes por função e cruzar com uma matriz que seja o resultado da interseção das responsabilidades dos trabalhadores e a sua avaliação na organização, com a autoavaliação do mesmo.

Bibliografia e Referências

Ali Alowayr and Atta Badi. (2014). *Review of Monitoring Tools for e-learning platforms.* Obtido de https://arxiv.org/ftp/arxiv/papers/1407/1407.2437.pdf

AMA - Agência para a Modernização Administrativa, I.P. (2017). *Simplex+*. Obtido em 14 de outubro de 2017, de Simplex: https://www.simplex.gov.pt/medidas

Athitakis, M. (Junho de 2014). *Data security: Keep a lid on it.* Obtido de Now associations: https://associationsnow.com/2014/06/data-security-keep-lid/

Blue, V. (2014). *Hacked: The six most common ways non-tech people fall victim.* Obtido de zdnet: http://www.zdnet.com/pictures/hacked-the-six-most-common-ways-non-tech-people-fall-victim/7/#photo

Caldwell, T. (12 de February de 2013). *Risky business: why security awareness is crucial for employees.* Obtido de The Guardian: https://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees

Comissão Europeia. (2017). *The Digital Economy and Society Index*. Obtido em 14 de Outubro, de https://ec.europa.eu/digital-single-market/en/desi

Cormier, D. (8 de Dezembro de 2010). *What is a MOOC?* Obtido em 15 de outubro de 2017, de https://www.youtube.com/watch?v=eW3gMGqcZQc

Costa, F., Santos , A., Silva , A., & Viana , J. (2015). *Experiências de Inovação Didática no Ensino Superior.* MEC.

Devaney, T. &. (2012). *Forbes*. Obtido de 5 Ways Small Businesses Can Protect Against Cybercrime: http://www.forbes.com/sites/capitalonespark/2012/12/17/5-ways-smallbusinesses-can-protect-against-cybercrime/

Dlamini, Z., & Modise, M. (2013). *Cyber security awareness initiatives in South Africa: a synergy approach.* Obtido em 3 de setembro de 2017, de Case Stud. Inf. Warf. Secur. Res. Teach. Stud : https://books.google.pt/books?hl=pt-

PT&lr=&id=vub26dKsmpIC&oi=fnd&pg=PA1&ots=BWaGeudlPR&sig=8mF3dE4wAsQMS1xD60pdFEwBlOQ&redir_esc=y#v=onepage&q&f=false

DOCEBO. (2016). *E-learning Market Trends & Forecast 2016 Report.*

ENISA - European Network and Information Security Agency. (2016). *Review of Cyber Hygiene practices.*

European Commission. (2017). *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks.* Brussels.

Hewitt, C. (2013, January). *For Privacy and Security, Use public Keys Everywhere.* Palo Alto, CA.

HM Government. (Março de 2014). *Cyber Security Skills: Business Prespectives and Government next steps*. Obtido em Setembro de 2017, de https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-securityskills-

HM Government. (2016). *NATIONAL CYBER SECURITY*. Obtido em agosto de 2017, de https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

IBM Security & Ponemon Institute. (2017). *2017 Cost of Data Breach Study.* Obtido de https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

K., R., & W., G. (2014). *The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture.* Obtido de K., R., & W., G. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture.

Latifa Ben Arfa Rabai, N. R. (2012). Quantifying Security Threats for E-learning Systems . *International Conference on Education and e-Learning Innovations* . Tunis, Tunisia.

Marsh. (2016). *Continental European Cyber Risk Survey: 2016 Report.*

Masadeh, M. (2012). *TRAINING, EDUCATION, DEVELOPMENT AND LEARNING: WHAT IS THE DIFFERENCE?* Obtido em 10 de outubro de 2017, de http://eujournal.org/index.php/esj/article/view/163/168

Nakamura, E. T., & Geus, P. L. (2007). *Segurança em redes cooperativos.* Obtido de https://books.google.pt/books?hl=pt-PT&lr=&id=AamSIJuLc34C&oi=fnd&pg=PA11&dq=Nakamura,+E.+T.,+%26+Geus,+P.+L.+(2007+).+Seguran%C3%A7a+em+redes+cooperativos.+S%C3%A3o+Paulo:+Novatec.&ots=Y0AkjefpP2&sig=8P_lr3i8S4R1kYFAac0A8B8sMBo&redir_esc=y#v=onepage&q&f=

National, I. o., & 800–50. (2003). Building an Information Technology Security Awareness and Training Program. Obtido de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

National, I. o., & 800–55. (s.d.). Security Metrics Guide for Information Technology Systems. Obtido de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55.pdf

National, I. o., & 800-56. (1998). Information Technology Security Training Requirements: A Role- and Performance-Based Model. Obtido de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-56.pdf

National, Institute of Standards and Technology Special Publication; 800–16. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* Obtido de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Paganini, P. (2013). *the importance of security requirements in designs of SCADA systems (PenTest auditing and standards 2012:06).*

Paulsen, C., & Tothsabel, P. (2016). *NISTIR 7621 Revision 1.* Obtido de NIST: https://beta.csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

Porto, U. d. (22 de Outubro de 2015). *Modelo pedagógico recomendado para MOOCs*. Obtido de https://elearning.up.pt/wp-content/uploads/2015/01/UTE-ModeloPedagogicoRecomendadoMOOC.pdf

Posthumus, S. &. (December de 2004). *Computers & Security.* Obtido de A framework for the governance of information security: http://dx.doi.org/10.1016/j.cose.2004.10.006

Presidência do Conselho de Ministros. (09 de 05 de 2014). Decreto-Lei n.º 69/2014.

Ranger, S. (2014). *NATO Updates Policy:Offers Members Article 5 Protection Against Cyber Attacks.* Obtido de http://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks

Republica Portuguesa- XXI Governo. (2017). *Incode2030*. Obtido em 14 de Outubro de 2017, de Incode2030: http://www.incode2030.gov.pt/

Rozensky, R. H., Grus, C. L., Nutt, R., Carlson, C., Eisman, E., & Nelson, P. (2015, January). A Taxonomy for Education and Training in Professional Psychology Health Service Specialties. *American Psychologist, Vol. 70*, pp. 21–32.

Sebe, M. (2014). The role of Education and Training in Intelligence. *UNIVERS STRATEGIC - Revistă Universitară de Studii Strategice Interdisciplinare, Nr. 2(18)*, pp. 60-64.

The Institute of Information Security Professionals. (2017). *IISP*. Obtido em setembro de 2017, de https://www.iisp.org/imis15/iisp/Accreditation/Our_Skills_Framework/iispv2/Accreditation/

Wise, E. H., & Cellucci, T. (2014). Using the Ethical Context to Enhance Practicum Training. *Vol. 8*, pp. 221–228.

Wyche, L. D. (2014, September-October). Training and Education Must Leverage Technology and Innovation. *Army Sustainment*, pp. 2-3.