
CYBERLAW
by CIJIC

EDIÇÃO N.º V – MARÇO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Antes de mais, salientarei uma novidade interna na organização do CIJIC. Desde final de Fevereiro de 2018, depois da assembleia geral, o Centro, passou a estar organizado, sob a Presidência do Professor Doutor Eduardo Vera-Cruz Pinto, coadjuvado por duas Vices, respetivamente, as Professoras Doutoras, Paula Vaz Freire e Raquel Alexandra Brízida Castro, e pelos vogais, Eugénio Alves da Silva e Nuno Teixeira Castro. Mais novidades surgirão em breve.

Feito o ponto de ordem inicial, e abertas as hostilidades, nesta nova edição, sem descurar a proximidade da entrada em vigor, em pleno, do *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados),* doravante, no acrónimo, RGPD, optamos por trazer a debate algumas tendências de futuro. Obviamente, quase todas com implicações, pungentes, quer ante o instrumento legislativo europeu em foco, quer, e acima de tudo, ante as formas mais tradicionais de relacionamento interpessoal e em sociedade.

Antecipando a tónica, o nosso futuro, já hoje muito intrincado com o digital, dependerá, no seu essencial, da contínua promoção de princípios e valores humanos que, ao longo dos tempos, nos foram acompanhando na evolução enquanto espécie racional. A compreensão, teoricamente mais facilitada até pelo dilúvio informacional

do presente, do conceito, *jus cogens*, de dignidade humana, deveria possibilitar a criação de uma consciência, atrever-nos-íamos a estribar de colectiva, global, do valor individual de cada vida humana em si considerada. Deveria. Porém, pouco disto tem vindo a suceder. As informações e notícias diárias têm vindo a sustentar precisamente um movimento díspar: uma sociedade hedonista mas profundamente egoísta, enamorada por um *surveillance capitalism*[1] reinante, sem espaço para a promoção da fundamentalidade de cada individualidade humana.

O poder inebriante, e sem precedentes na nossa história civilizacional, detido por algumas organizações, denominadas de *tech-giants*, tem rompido as estruturas sociais, políticas, comerciais e, até, tecnológicas. Qual a origem de tão avassalador poder disruptivo destas organizações, destes *tech-giants*?

Em parte, grande, o *graal* destes *tech-giants* deriva de todo o *dilúvio informacional* que percorre a rede. Numa relação de *win-win*, a "*oferta inocente"* de serviços, prosaicamente assimilados como *grátis*, em troca dos nossos dados pessoais, é obnóxia para o indivíduo. Mas profundamente fluída no garante de volumosos acréscimos de capital financeiro, e por conseguinte, de poder, para estas organizações. Bruce SCHNEIER[2], a este propósito, sintetiza de forma lapidar: «*Companies like Facebook and Google offer you free services in exchange for your data. Google's surveillance isn't in the news, but it's startlingly intimate. We never lie to our search engines. Our interests and curiosities, hopes and fears, desires and sexual proclivities, are all collected and saved. Add to that the websites we visit that Google tracks through its advertising network, our Gmail accounts, our movements via Google Maps, and what it can collect from our smartphones. That phone is probably the most intimate surveillance device ever invented. It tracks our location continuously, so it knows where we live, where we work, and where we spend our time. It's the first and last thing we check in a day, so it knows when we wake up and when we go to sleep. We all have one, so it knows who we sleep with. »* Sim, *o smartphone é provavelmente o dispositivo, mais íntimo,* pessoalíssimo mesmo, *de vigilância jamais inventado.* Acompanha-nos permanentemente, 24h/7d, 365d/ano, qual extensão do nosso corpo.

1 https://www.amazon.com/Age-Surveillance-Capitalism-Future-Frontier/dp/1610395697
2 https://www.schneier.com/

E sempre a debitar informação para alguém, transformando-nos no escravo, informacional, do...objecto. Curioso, não?

De facto, disfarçado de *pot-pourri* de intimidade, proximidade e confiança cega, os gigantes tecnológicos têm-nos orientado a um estado de, *quase-completa*, submissão a variadíssimas formas de engenharia social, perfumada por formas competentes e persuasivas de direcção comportamental, categoricamente personalizadas e orientadas para fazermos *algo ao serviço de alguém*; uma verdadeira manipulação individualizada orientada pelo perfil de cada um, de previsão e controlo do nosso comportamento. Fácil de conseguir quando em posse de tão valiosa informação que vamos cedendo, sem limites. Sem conhecimento. Sem oposição. Shoshana ZUBOFF[3], arroja duas questões sufocantes, a cada um de nós, nesta era digital da sociedade informacional: "*Mestre ou escravo*?", "*Casa ou exílio*?". (Conseguiremos responder?)

Os desafios para o futuro da humanidade travam-se. Fugir, ou recear tal, não poderá ser a resposta. Nesta conjuntura crítica, nesta *nova fronteira do poder*, o confronto entre o vasto poder dos gigantes tecnológicos versus os dos governos (enquanto representantes da nossa comunidade colectiva), atira-nos, sem pudor, para um difícil campo de escolhas, civilizacionais diria. O futuro da humanidade tem espaço para a autonomia individual e para os direitos fundamentais? Ou assistiremos impávidos ao desabrochar de novas e sofisticadas formas de desigualdade social? O *el dorado* da era digital possibilitará o fortalecimento dos direitos fundamentais individuais e a sua democratização globalizante? Ou assistiremos impávidos à instrumentalização do indivíduo, segmentado em objecto de informações em meras *strings de bits*, coisificado, servil ao *surveillance capitalism*?

Nesta insolência de questões, e uma vez aqui chegados, foi nossa intenção suscitar a comunidade académica e empresarial a problematizar algumas teorias de resposta. Não assumindo o absolutismo das coisas, o resultado presente é, a nosso ver, profundamente satisfatório. Neste nosso *pot-pourri* que agora publicamos, carreamos *big data*; segurança da informação; regulamento geral de protecção de dados; veículos autónomos e inteligentes; *criptocontratação*; contratos automatizados e contratos

3 http://www.shoshanazuboff.com/

inteligentes; dados pessoais e direitos fundamentais; e, mecanismos de cooperação e coerência no tratamento de dados pessoais.

Agradecidos pelo esforço e pelo trabalho, cumpre-me, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, endereçar um especial reconhecimento a cada um dos autores.

Um sentido e imenso Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 30 de Março de 2018

Nuno Teixeira Castro

DOUTRINA

MODELO INTEGRADO DE ATIVIDADES PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS

JOSÉ MARTINS

HENRIQUE SANTOS

JORGE CUSTÓDIO

&

RUI SILVA [1]

1 jose.carloslm@gmail.com, Academia Militar / CINAMIL, FeelSec Consulting
hsantos@dsi.uminho.pt, Dep. Sistemas de Informação, Universidade do Minho
jorge.filipe.custodio@gmail.com, FeelSec Consulting
& rs.beja@gmail.com, Instituto Politécnico de Beja / UbiNET

RESUMO

Este artigo propõe um modelo que identifica e agrupa em seis dimensões as atividades que contribuem, nas organizações, para a Gestão da Segurança da Informação, a Cibersegurança e a Proteção de Dados Pessoais. O Modelo está orientado para apoiar a atividade profissional dos *Chief Information Security Officer* (CISO), dos Encarregados de Proteção de Dados, dos Consultores e Gestores de Projetos que procuram possuir uma visão holística e integrada destas temáticas. O modelo proposto tem uma abordagem sistémica, na qual se procuram identificar métodos, técnicas e ferramentas de diferentes domínios científicos para a gestão destas temáticas. É suportado numa revisão de literatura, na experiência dos autores resultante da sua atividade académica, auditorias e implementação de Sistemas de Gestão de Segurança da Informação, bem como de projetos de *desenho* e implementação de Sistemas de Informação (SI). É um trabalho de *Design Science* em progresso, através do qual irá ser validado o modelo proposto através da aplicação de um questionário a especialistas *e* da utilização do método de investigação *Action Research*. Como principal resultado obtido deste estudo, salienta-se o modelo de atividades integrado para Gestão de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais.

Palavras-Chave: Segurança da Informação; Cibersegurança; Proteção de Dados Pessoais; Modelo Integrado de Segurança; Competências de um CISO.

1. INTRODUÇÃO

Na atual Sociedade em Rede, onde as ameaças à informação e aos Sistemas de Informação (SI) são permanentes e evolutivas, é necessário que os atores com responsabilidades nos processos de decisão relativos à Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais nas organizações (e.g., CIO, CISO) possuam uma visão de conjunto e integrada. Existe ainda, um conjunto de especialistas que necessitam de um modelo que lhes permita sistematizar e estruturar as atividades e o conhecimento relacionados com as tarefas profissionais que, diariamente, lhe são solicitadas no âmbito destas temáticas.

A multidimensionalidade do problema, bem como a sua complexidade, exige um modelo que reflita uma abordagem multidisciplinar e sistémica. Deste modo, foram consideradas, para o *desenho* do modelo, as seguintes dimensões: (i) *Organização*; (ii) *Adversário*; (iii) *Capacidade de Proteção*; (iv) *Planeamento*; (v) *Gestão Operacional*; (vi) *Formação, Sensibilização e Treino* (Figura 1).

Figura 1: Modelo Integrado de Segurança

Cada uma das dimensões referenciadas na Figura 1 agrega um conjunto de sub-dimensões, que representam atividades profissionais nucleares para a gestão da segurança, que, direta ou indiretamente, contribuem para garantir a confidencialidade, integridade e disponibilidade da informação processada, transmitida e armazenada.

Estas seis dimensões resultam de uma abordagem *bottom-up*, predominantemente interpretativa, com base na análise e síntese documental das referências indicadas para cada uma das sub-dimensões (Tabelas 1 a 6). Esta conceptualização é ainda suportada na experiência dos autores resultante: (i) da sua atividade académica; (ii) da execução de auditorias e implementação de Sistemas de Gestão de Segurança da Informação (e.g., ISO/IEC 27001); (iii) da formulação de projetos de *desenho* e implementação de SI; (iv) bem como na administração de infraestruturas na realização de testes de intrusão.

Possivelmente existem sub-dimensões/atividades não identificadas no modelo proposto, mas acredita-se que todas as referenciadas neste artigo são as mais relevantes, quer no planeamento ou implementação, quer na melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI), que, simultaneamente, se interligue com a Cibersegurança e a Proteção de Dados Pessoais.

Constata-se, através da revisão de literatura, a existência de diversas abordagens relativas à Gestão da Segurança da Informação e à Cibersegurança, sendo comum a todas elas a necessidade de realizar uma identificação e avaliação de riscos dos ativos e dos processos de negócio, seguido do endereçamento dos mesmos através da implementação de controlos de segurança de diferentes classes (e.g., tecnológicos, físicos, administrativos) em função das estratégias para a gestão das ameaças. No entanto, mesmo com níveis de maturidade elevados nos controlos implementados é necessário, ainda, ter planos de contingência (e.g., de *disaster recovery*), pois o risco residual permanecerá e o incidente certamente que ocorrerá, mais cedo ou mais tarde.

Estas abordagens, têm por suporte, na sua maioria, o modelo de gestão conhecido por PDCA *(Plan, Do, Chek e Act)*, o qual procura, em permanência, a melhoria contínua do SGSI. O modelo proposto neste artigo identifica atividades que permitem instanciar estas fases, embora não forneça, ainda, um método que as permita relacionar.

Da análise das abordagens de segurança ao nível organizacional identificam-se como principais dimensões de segurança a: (i) Física e Ambiental; (ii) Humana; (iii) Tecnológica; (iv) Organizacional; em função das quais os principais controlos de segurança podem ser implementados e geridos.

De forma a descrever o modelo proposto o artigo está estruturado em oito seções. Na primeira enquadra-se o problema. Posteriormente, na segunda analisam-se as principais atividades necessárias para conhecer a *Organização*. A terceira seção foca-se nas possíveis ações maliciosas / métodos de ataque do *Adversário* e a quarta nas *Capacidades de Proteção* disponíveis atualmente. Na quinta discutem-se as atividades que contribuem para o *Planeamento*. Seguidamente, na sexta seção descrevem-se as atividades de *Gestão Operacional e* na sétima as centradas na *Formação, Sensibilização e Treino* dos colaboradores da organização. Por fim, na oitava apresentam-se os principais resultados da investigação, as limitações do estudo e alguns dos possíveis os trabalhos futuros a realizar.

2. A ORGANIZAÇÃO

Para realizar a gestão dos controlos de Segurança implementados, ou a aplicar, no âmbito de um SGSI, da cibersegurança e proteção de dados pessoais, é necessário, em primeiro lugar, conhecer em detalhe a Organização. Esta atividade passa, fundamentalmente, por conhecer: (i) o seu ambiente envolvente; (ii) a cultura institucional; (iii) o modelo de gestão; (iv) os processos de negócio; (v) a

arquitetura dos Sistemas de Informação; (vi) e, ainda, os dados e a informação (e conhecimento) associados aos processos de negócio (Figura 2).

Figura 2: Conhecer a Organização

O conhecimento do ***Ambiente Envolvente*** permite identificar, de forma macro, algumas das principais ameaças que pendem sobre os ativos da organização. Em relação à ***Cultura Organizacional*** é necessário considera-la na gestão da mudança associada à execução das atividades de segurança, tendo em consideração os comportamentos predominantes dos funcionários da Organização e dos colaboradores externos.

Por outro lado, conhecer o ***Modelo de Gestão*** implementado na organização (e.g., Sistema de Gestão Integrado baseado na ISO/IEC 9001), permitirá, mais facilmente, alinhar os controlos de segurança a implementar com os objetivos estratégicos e operacionais do negócio. Simultaneamente, a análise dos ***Processos de Negócio*** da cadeia de valor, permite identificar a informação nuclear para o negócio e os ativos críticos a proteger.

É, ainda, necessário conhecer a ***Arquitetura dos SI*** da Organização, onde se inclui a infraestrutura tecnológica de suporte (i.e., a sua rede de computadores),

que é um elemento essencial no processo de conhecer as respetivas vulnerabilidades. E, por fim, é determinante conhecer os ***Dados / Informação*** que integram os processos de negócio, considerando-se fundamental identificar o seu ciclo de vida, o seu valor e a sua classificação de segurança.

Nas sub-dimensões que contribuem para a análise da Organização podem-se utilizar Métodos, Técnicas e Ferramentas (MTF) (Tabela 1) com origem em outras áreas do conhecimento (e.g., Gestão, Sistemas de Informação, Sociologia, Psicologia), de validade científica ou profissional comprovada, que podem ser úteis ao especialista no *desenho* e na gestão de um SGSI, o que reforça a necessidade dos especialistas nestas temáticas terem uma visão holística e multidisciplinar.

Tabela 1: Conhecer a Organização

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Ambiente Envolvente	Técnicas de Gestão (e.g., PESTAL, PORTER, SWOT)	(Teixeira, 2005)
Cultura Organizacional	Tipologia de Culturas (e.g., Comunidade)	(Robbins, 2002)
Modelo de Gestão	Sistema de Gestão integrado	(Teixeira, 2005); (ISO/IEC 9001, 2015)
Processos de Negócio	Modelação de Processos (e.g., BPMN)	(Weske, 2007)
Arquitetura de SI	Framework de Zackman; TOGAF	(Greefhorst, Danny and Proper, 2011); (Laudon e Laudon, 2006); (Turban, Rainer e Potter, 2003)

Dados, Informação e Conhecimento	Ciclo de Vida da Informação; Valor Informação; Classificação da Informação	(Gleick, 2006); (Nonaka e Takeuchi, 1995); (Santos e Isabel, 2006)

Nos MTF referenciados na Tabela 1 e posteriores (Tabelas 2 a 6), a preocupação principal dos autores é deixar ao leitor *referências* sobre estas temáticas. Conhecer a Organização em detalhe permite, certamente, aumentar a eficiência e eficácia do SGSI implementado, pois exige-se uma *Arquitetura de Segurança* integrada com o seu modelo de negócio.

3.O ADVERSÁRIO

Após a análise da Organização é necessário conhecer o Adversário (Figura 3). Esta atividade passa fundamentalmente por conhecer: (i) o campo de ação onde este atuará; (ii) os principais atores que o podem tipificar; (iii) os seus possíveis vetores e métodos de ataque; (iv) as vulnerabilidades que este procurará explorar; (v) as técnicas de simulação de métodos de ataque que permitem treinar as modalidades de ação de um adversário, de modo a selecionar a forma mais eficiente e eficaz de aplicação dos controlos para a proteção da Organização; (vi) a doutrina associada às *Computer Network Operations, especialmente a militar*, pois estas representam, em termos de intenção e capacidade de um hipotético adversário, o pior cenário defensivo para as Organizações, num possível ambiente conflitual.

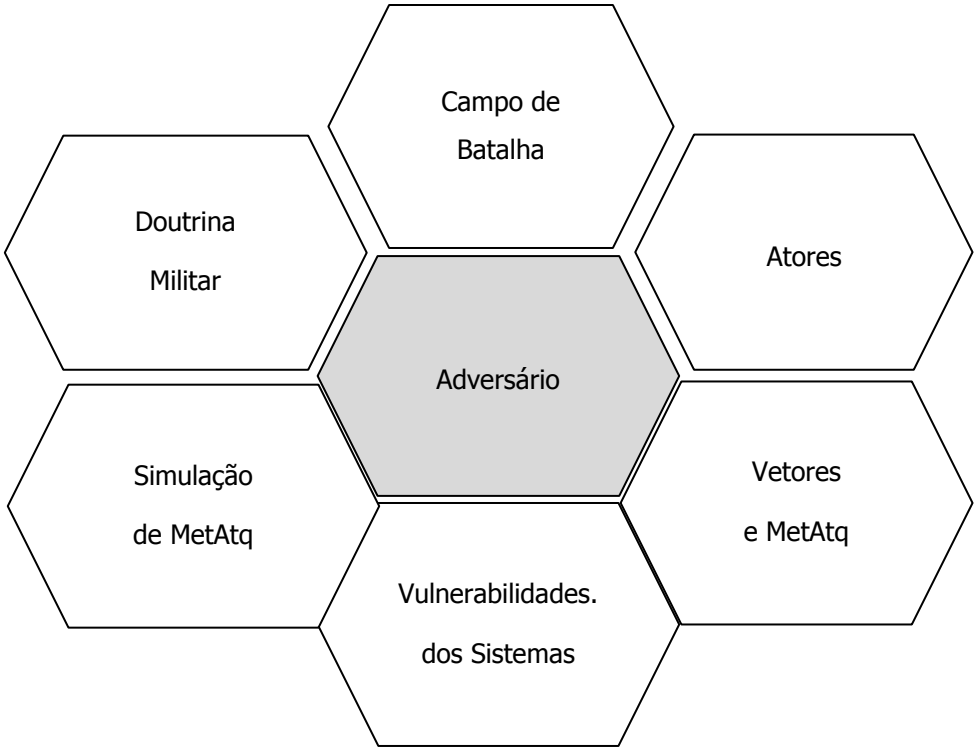

Figura 3: Conhecer o Adversário

Para poder endereçar os riscos de Segurança da Informação e Cibersegurança, ou numa perspetiva bélica, ter capacidade de fazer face aos métodos de ataque de um adversário é necessário conhecer em primeiro lugar o ***Campo de Batalha***, i.e., o ambiente onde este atua. Consequentemente, é essencial ter conhecimento sobre o funcionamento e estrutura das redes de computadores, da Internet, componentes aplicacionais existentes e, ainda, das linguagens de programação e suas vulnerabilidades.

É, também, importante ter a perceção de quais poderão ser os principais ***Atores*** a interagir de forma maliciosa com a Organização. Subsequentemente, é necessário conhecer os seus níveis de atuação (chamados eixos de aproximação do Inimigo, em doutrina militar) e os possíveis ***Métodos de Ataque*** (ações e ferramentas utilizadas), através dos quais procurarão explorar as vulnerabilidades identificadas relativamente aos ativos da Organização.

Estas ações numa Organização podem ser executadas segundo três níveis de ataque principais: o físico, o humano e o da infraestrutura tecnológica, que são suscetíveis de poder comprometer as propriedades fundamentais de segurança da informação, i.e., a confidencialidade, integridade e disponibilidade.

A execução de um método de ataque, i.e., de uma ação ou conjunto de ações maliciosas por parte de um adversário, visa explorar uma ou mais vulnerabilidades (debilidades dos Sistemas, resultantes do seu desenho, parametrização, administração ou utilização) de um determinado Sistema. Estes métodos de ataque podem e devem ser simulados pelas Organizações, em ***ambientes controlados***, de forma a testar soluções de segurança, sensibilizar e treinar os colaboradores a responder a incidentes, bem como validar os seus planos de contingência (e.g., *Disaster Recovery*).

Uma análise mais detalhada em termos da possível atuação de um adversário, i.e., das suas possíveis modalidades de ação, pode ser complementada através do estudo da ***Doutrina Militar*** de Operações de Informação, onde as *Computer Network Operations*, são uma das capacidades fundamentais ou de *Frameworks* de Testes de Intrusão.

Se, numa primeira iteração, os requisitos de segurança da Organização associados às propriedades de Segurança da Informação e os ativos críticos que fazem parte dos processos de negócio são essenciais para as organizações orientarem o planeamento, uma segunda iteração é fundamental a identificação dos vetores e métodos de ataque, procurando, se possível, identificar as modalidades de atuação do adversário mais prováveis (com maior probabilidade de ocorrer) e as de maior impacto.

Ao nível físico, podem considerar-se, a título exemplificativo, ações maliciosas sobre as instalações físicas, os equipamentos (e.g., o *hardware)*, os sistemas de suporte (e.g., sistema de energia elétrica), os documentos em suporte físico (e.g., sabotagem, roubo) e as próprias pessoas (e.g., especialistas com funções essenciais na organização).

É, ainda, fundamental salientar a importância da prevenção de catástrofes naturais (e.g. pandemias, tremores-de-terra) ou desastres (e.g. incêndios, inundações), de forma a garantir, também, a Segurança da Informação (e.g., disponibilidade). Estes incidentes, a ocorrerem, tem consequências sobre determinados componentes dos SI, nas instalações ou nos respetivos processos de negócio (inclui os recursos humanos).

Ao nível da infraestrutura tecnológica, as ações maliciosas podem ser executadas sobre aplicações diversas (e.g., Sistemas Operativos, Bases de Dados). Estas ações possibilitam, também, alterar o funcionamento da sua rede de computadores, através de acesso interno, ou externo (e.g., através da Internet), e explorar vulnerabilidades dos serviços implementados.

Finalmente, ao nível humano, deve dar-se especial atenção às ações que possibilitem: (i) manipular os colaboradores (internos e externos) da Organização (e.g., ataques de *phishing*); (ii) criar falsas perceções nos decisores para uma determinada situação; (iii) e ainda alterar os processos de decisão implementados.

Existem, também, nesta dimensão alguns MTF que podem ser utilizadas para obter um conhecimento mais pormenorizado do adversário e que estão referenciadas na Tabela 2.

Tabela 2: Conhecer o Adversário

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Campo de Batalha	Redes de Computadores Públicas e Privadas (protocolo TCP-IP, ativos de rede).	(Kurose e Ross, 2010); (Knapp e Langill, 2015); (Correia e Sousa, 2010)
Atores	Taxonomias de Atores (e.g., Intel TARA)	(Carr, 2012); (Andress e Winterfeld, 2011); (Waltz, 1998)

Vetores e Métodos de Ataque	Frameworks de MetAtq (e.g., CAPEC, OWASP)	(Pfleeger e Pfleeger, 2012); (Gregg, 2006); (Wantson, Mason e Ackroyd, 2014)
Vulnerabilidades dos Sistemas	Taxonomias de Vulnerabilidades (e.g., CVS, NVD)	https://nvd.nist.gov; http://www.cve.mitre.org (consultados em 27 de Dezembro de 2017)
Simulação de Métodos de Ataque	Frameworks de Testes de Intrusão, Técnicas (e,g., árvores de ataque, cenarização), Ferramentas (e.g., KALI)	(NIST 800-115, 2008); (Shostack, 2014); Martins, Santos, Nunes and Silva (2012b)
Doutrina Militar	Operações de Informação e *Computer Network Operations*	(FM 3-13, 2003); (JP 3-13, 2012); (JP 3-12, 2013); (FM 3-38, 2014)

Após abordar a perspetiva do adversário, identificam-se na próxima seção as principais capacidades de proteção atualmente disponíveis, que permitem à Organização garantir a Segurança da Informação, Cibersegurança e a Proteção de Dados.

4.AS CAPACIDADES DE PROTEÇÃO

Após conhecer a Organização e o Adversário, é necessário ter uma visão atual das *Capacidades de Proteção* disponíveis, i.e., o "*Estado-da-Arte"* (Figura

4) e que passa fundamentalmente por conhecer: (i) os princípios e postulados da segurança; (ii) as principais disciplinas académicas de referência que suportam estas temáticas; (iii) as tecnologias de segurança existentes; (iv) as normas internacionais ou nacionais e as certificações reconhecidas pela Industria; (v) a legislação e a regulamentação da área de negócio da Organização com obrigatoriedade jurídica de cumprimento; (vi) e ainda a interligação entre capacidades Defensivas vs. Ofensivas, ou seja, que controlos de segurança aplicar para métodos de ataque específicos.

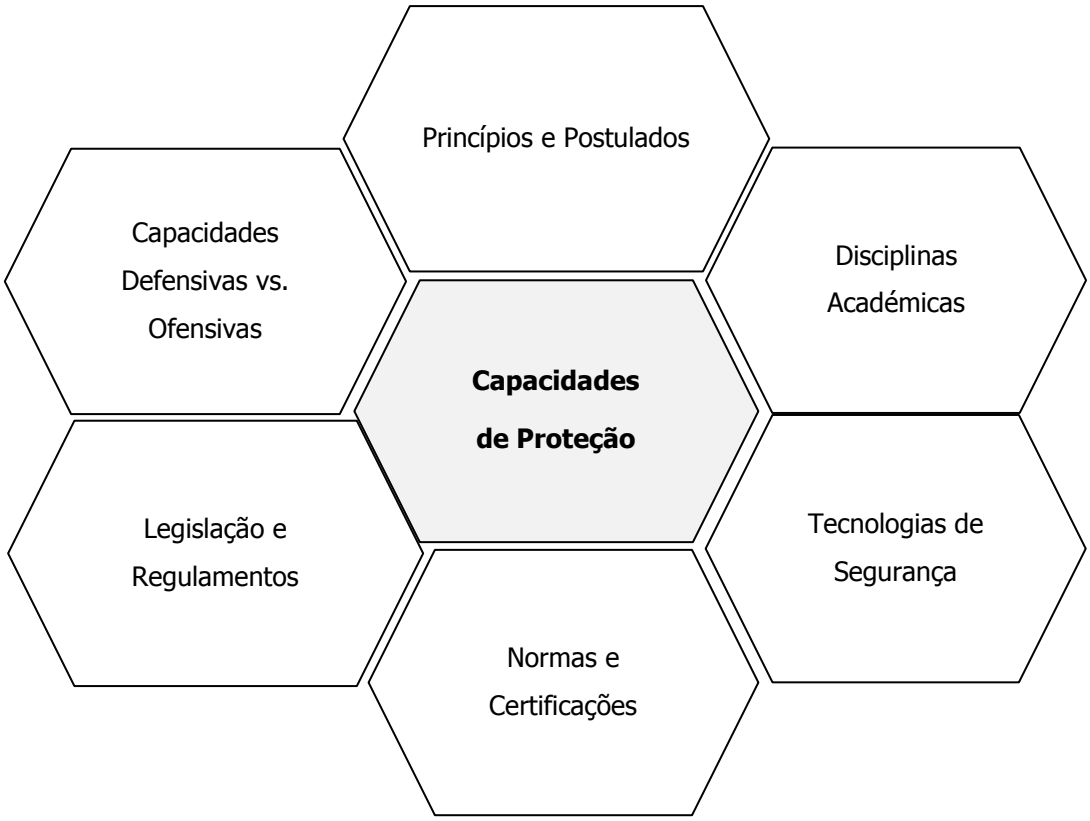

Figura 4: Conhecer as Capacidades de Proteção

Em primeiro lugar deve-se orientar a Segurança da Informação e a Cibersegurança por um conjunto de ***Princípios e Postulados*** que são suportados na experiência dos especialistas e unanimemente aceites, dos quais se salientam: (i) *"a defesa em profundidade" (i.e., múltiplas camadas de proteção); (ii) "a necessidade de conhecer"; (iii) e "o mínimo privilégio".*

É, também, obrigatório considerar-se o conhecimento das ***Disciplinas Académicas*** de referência que suportam estas temáticas, como sejam, e principalmente: (i) a criptografia; (ii) a segurança de redes de computadores; (iii) a segurança da Internet; (iv) e a segurança no *software*.

Por outro lado, é necessário considerar a utilização de boas práticas ou recomendações de segurança já aceites pelos especialistas e que se encontram muitas delas já refletidas em ***Normas*** Internacionais (e.g., ISO / IEC 27001, ISO / IEC 27032), Nacionais (e.g., NIST 800-53 / EUA), ou em ***Certificações*** (e.g., CISSP). Deve, ainda, garantir-se a utilização de tecnologias que atualmente são *Commodities de Segurança* (e.g., *firewall*, antivírus).

É, ainda, fundamental considerar os ***Regulamentos*** do setor de negócio da Organização, bem com a ***Legislação*** em vigor no País em que exerce atividade. Atualmente um dos aspetos mais relevantes e obrigatórios para as Organizações com sede na União Europeia é o cumprimento do Regulamento Geral de Proteção de Dados (EU 2016 / 679), sendo critico, em termos de segurança, o cumprimento do Art.º 32.º (Segurança do Tratamento).

Um aspeto nuclear nesta dimensão é a capacidade de ***Interligar as Modalidades de Ação*** do adversário, ou seja, os seus métodos de ataque, com controlos de Segurança da Informação ou Cibersegurança, procurando, continuamente, melhorar a sua eficiência e eficácia, através da avaliação do nível de maturidade destes para endereçar os riscos identificados pela Organização. Existem alguns MTF que estão disponíveis para apoiar o *desenho* e implementação de um SGSI e que são referenciadas na Tabela 3.

Tabela 3: Conhecer as Capacidades de Proteção

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Princípios e Postulados	Defesa em Profundidade, Necessidade de Conhecer, Mínimo Privilégio	(NIST 800-27, 2004); (Dhillon, 2007);

Tabela 3: Conhecer as Capacidades de Proteção		
Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
		(Pfleeger e Pfleeger, 2007); (Smith, 2013); (Whitman e Mattord, 2012)
Disciplinas Académicas	Criptografia, Segurança de SI; Segurança de Redes, Segurança da Internet, Segurança no Software	(Stallings, 2011); (Dhillon, 2007); (Zúquete, 2007); (Touhill e Touhill, 2014); (Correia e Sousa, 2010)
Tecnologias de Segurança	Firewall, Antivírus, SIEM, Gestão de Identidades e Acessos	(Venter e Eloff, 2003)
Normas e Certificações	ISO / IEC 27001, NIST 800 – 53, Frameworks de Cibersegurança, CISSP	(ISO 27001, 2013); (NIST 800 – 53, 2013); (ISO 27032, 2012); (CISSP_CKB, 2013); SANS (2013); (Martins and Santos, 2010)
Legislação e Regulamentos	Lei da Cibercriminalidade, Regulamente de Proteção de Dados, Legislação de Segurança Nacional	(Fazendeiro, 2017)

Tabela 3: Conhecer as Capacidades de Proteção		
Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Capacidades Defensivas vs. Ofensivas	Modelos de Apoio à Decisão (e.g., Teoria dos Jogos), Cenarização (e.g., Análise Morfológica Geral)	(Martins, 2015); (Ritchey, 2010)

A revisão de literatura realizada, permitiu identificar métodos e normas orientados para: (i) a gestão do risco da Segurança da Informação (e.g. OCTAVE, ISO/IEC 27005); (ii) normas de certificação e boas práticas de gestão de Segurança da Informação e de SI (e.g. ISO/IEC 27001, ISO/IEC 27002, NIST 800-53); (iii) e normas e boas práticas de segurança com foco tecnológico (e.g. ISO/IEC 13335-4, NIST 800-54). Existem, também, normas orientadas à certificação do produto ou Sistema (e.g. ISO/IEC 15408) e normas para avaliar a maturidade dos processos de segurança de uma organização (e.g. ISO/IEC 21827).

Por fim, identificam-se, também, normas da Indústria que embora mais orientadas aos processos de negócio (e.g. CobiT5) e à gestão das TI (e.g. ITIL V3, ISO/IEC 20000), que refletem uma preocupação com a Segurança da Informação. Salienta-se, ainda, a possível aplicação dos controlos referenciados em algumas das principais abordagens de Cibersegurança, como sejam: (i) as recomendações da ISO / IEC 27032; (ii) a *framework* de Cibersegurança do NIST; (iii) as boas práticas da ENISA; (iv) ou os 20 controlos de Ciberdefesa indicados pela SANS, muitos dos quais também sugeridos pelas abordagens de Segurança da Informação atrás referenciadas.

Nas abordagens de Segurança da Informação e Cibersegurança em apreço, é comummente aceite que as propriedades fundamentais da segurança da informação são a confidencialidade, a integridade e a disponibilidade, sendo necessário garantir que tais propriedades não são afetadas: (i) por ações maliciosas ou negligentes realizadas por elementos externos ou internos à Organização; (ii)

pela ocorrência de catástrofes naturais ou desastres internos; (iii) ou pela execução de eventos não previstos ocorridos nos ativos tecnológicos implementados (e.g., falhas).

Em termos da proteção de dados, o regulamento no Art.º 32º - Segurança do Tratamento, refere a importância de aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco e a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. Certamente que as abordagens identificadas anteriormente terão os controlos necessários e, eventualmente, suficientes para garantir esta proteção.

Esta dimensão permite conhecer algumas das principais abordagens para a gestão da Segurança da Informação e Cibersegurança *(Estado-da-Arte)*, as tecnologias de segurança disponíveis e ainda as obrigações legais e regulamentares das organizações.

5.O PLANEAMENTO

Após conhecer a Organização, as capacidades do Adversário e as Capacidades de Proteção existentes, está-se na posse dos elementos mais relevantes para iniciar o Planeamento de um SGSI (Figura 5), o qual pode ser definido como o processo de determinar, antecipadamente (inclui previsão), o que deve ser feito, por quem, quando e como fazê-lo. Nesta dimensão é fundamental saber: (i) analisar sistemas complexos; (ii) especificar requisitos e modelar processos; (iii) identificar, avaliar e estimar riscos; (iv) efetuar o *design* de políticas de segurança; (v) e de planos de contingência; (vi) e, ainda, gerir projetos (projetar o planeamento na implementação, através de um método).

Figura 5: Planeamento da Segurança

Uma primeira atividade fundamental, é a capacidade de efetuar a ***Análise de Sistemas*** complexos, i.e., com múltiplas variáveis, e de definir com rigor os ***Requisitos*** que um SGSI deve ter, bem como efetuar o *desenho* do seu processo de gestão operacional e a interligação com todos os outros processos de negócio da organização.

Outra atividade central no planeamento é a ***Identificação e Avaliação de Riscos*** dos ativos críticos para o negócio, de modo a, posteriormente, se implementar o plano de tratamento.

Esta atividade deve ser o centro de gravidade do planeamento, pois permite interligar as principais variáveis do problema (ameaças, ativos, vulnerabilidades, controlos).

É nuclear que o SGSI seja suportado por um conjunto de ***Politicas de Segurança da Informação*** (e.g., Politica de Segurança da Informação) e ***Planos de Contingências*** (e.g., *Disaster Recovery*). Deve, ainda, garantir-se no

planeamento que a implementação dos controlos do SGSI seja realizada de acordo com as melhores práticas de ***Gestão de Projetos***, testando, se possível, a sua implementação em ambiente de desenvolvimento e qualidade, antes da sua implementação em ambiente de produção.

Um aspeto a ter em conta na criação das políticas / planos e na gestão de projetos é a existência de uma linguagem comum (e.g., taxonomia) que permita que diferentes atores tenham o mesmo entendimento do problema.

Para efetuar o planeamento existe um conjunto de MTF (Tabela 4) que poderão apoiar, e cuja indicação neste artigo resulta da aplicação das mesmas pelos autores em diversos projetos empresariais, que permitiram suportar a fase de análise e desenho de processos de Segurança da Informação ou Cibersegurança.

Tabela 4: Métodos, Técnicas e Ferramentas de Planeamento

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Análise de Sistemas	Questionários, *Focus Group*, Entrevistas, Diagramas de Causa-Efeito	(Eaton, Redmayne and Thordsen, 2007); (Liamputtong, 2011); (Remenyi, 2012)
Requisitos e Modelação de Processos	*UML - Use Cases*, BPMN	(Silva e Videira, 2005); (Wiegers e Beatty, 2013)
Gestão do Risco	Técnicas qualitativas ou quantitativas	(ISO 31000, 2012); (ISO 31010, 2016); (ISO 27005, 2011)

Políticas de Segurança	Politica de Segurança da Informação, Políticas Técnicas, Instruções Operacionais	(Sá Soares, 2004); (CISSP_CBK, 2013); (NIST 800-18, 2006)
Planos de Contingência	Incidentes e Problemas, Disaster Recovery, Continuidade de Negócio, Gestão de Crises	(Whitman, Mattord e Green, 2014); (NIST 800-34, 2010); (ISO 22301, 2012)
Gestão de Projetos	PMBOK, APMI, SCRUM	(PMBOK, 2013); (Hermarij, 2013); (Sutherland, 2014)

Após planear, é necessário implementar o SGSI ("*To Be*"), o qual deve ser realizado de forma iterativa e em que, na maioria das vezes, se utilizam controlos de segurança que já estão implementados na Organização, os quais são identificados e avaliados nas atividades de análise da Organização ("*As Is*"). Um aspeto fundamental é, ainda, considerar, desde o início de um projeto para desenvolvimento de um produto, processo, ou serviço, a Segurança da Informação. Após a implementação de um SGSI é fundamental a sua Gestão Operacional, dimensão esta que será abordada na próxima seção.

6. A GESTÃO OPERACIONAL

As tarefas principais da Gestão Operacional são: Planear (atividade descrita anteriormente), Organizar, Dirigir e Controlar todos os esforços a realizar em todas as áreas / processos de negócio e a todos os níveis da Organização (estratégico, tático e operacional), a fim de garantir os seus requisitos de Segurança. Nesta dimensão identificam-se como principais sub-dimensões: (i) a liderança digital; (ii) a monitorização e as auditorias; (iii) a gestão das Tecnologias de Informação; (iv) a gestão da *framework* de controlos de segurança implementados; (v) a resposta a incidentes e recuperação de desastres; (vi) e a continuidade de negócio e gestão de crises (Figura 6).

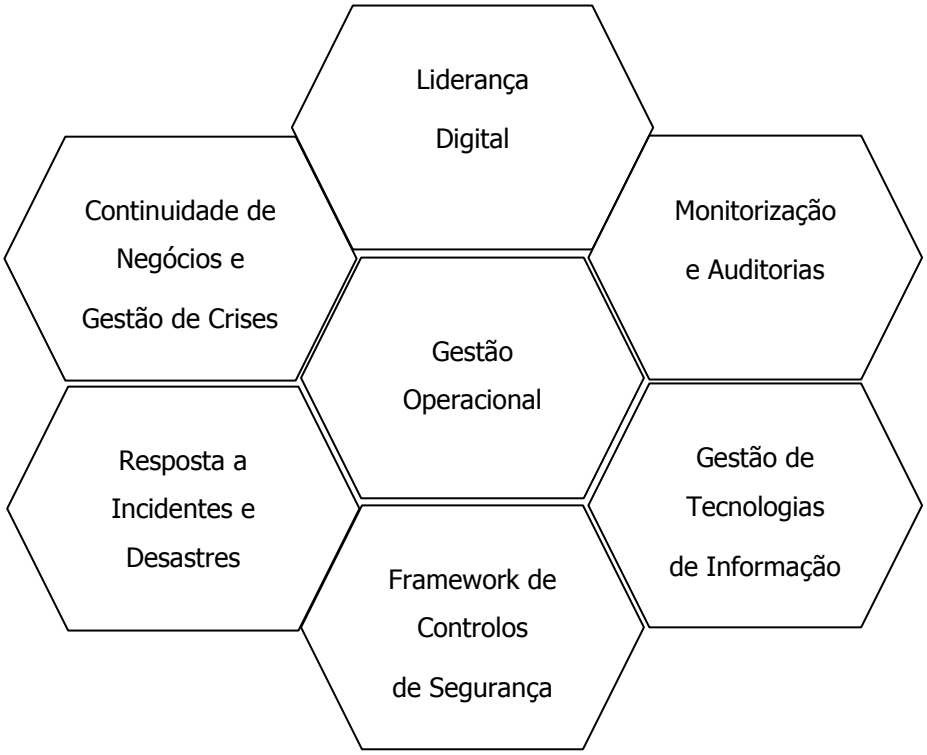

Figura 6: A Gestão Operacional da Segurança

Um dos aspetos fundamentais é a ***Liderança Digital***, que passa fundamentalmente pela gestão dos elementos que gerem a segurança ("Quem Controla o Polícia?"). É necessário também que os decisores considerem nas suas atividades de gestão novas formas de liderar em virtude das suas equipas de TI / Segurança serem na maioria das vezes constituídas por equipas de *Outsourcing*, a trabalhar remotamente através de ambientes colaborativos (equipas virtuais), com

limitadas relações pessoais entre os elementos da equipa, os quais na maioria das vezes tem diferentes nacionalidades, com os constrangimentos que daí resultam.

Outro aspeto essencial é a ***Monitorização e Auditoria*** das ações realizadas sobre os dados / informação armazenada, transmitida ou processada na organização, especialmente a de valor mais elevado (e.g., dados pessoais). Uma possível solução pode passar por possuir: (i) um *Security Information and Event Management*, que centralize e correlacione todos os eventos de segurança da Organização; (ii) e um sistema de gestão de identidades e acessos, que garanta às Organizações, identidades digitais únicas associadas aos colaboradores, em todos os Sistemas, e com perfis de acesso bem definidos.

É, também, importante uma eficiente ***Gestão das Tecnologias de Informação*** da Organização, com especialmente preocupação para a sua disponibilidade e capacidade de suportar os seus processos de negócio. A correta aplicação de boas práticas de gestão das TI permite endereçar muitos dos riscos de Segurança da informação e Cibersegurança.

A componente operacional, ou seja, as operações do dia-a-dia, passam pela gestão de uma ***Framework de Controlos de Segurança*** implementados, cuja estrutura se sugere estar orientada, fundamentalmente, pelas dimensões: (i) Organizacional; (ii) Física e Ambiental; (iii) Humana; (iv) e Tecnológica; que devem proteger dos principais níveis de atuação de um adversário e dos seus métodos de ataque. Nesta *framework* deve-se procurar uma integração de controlos que garanta o propósito de prevenir, detetar, deter, desviar, recuperar e reagir, face aos riscos identificados na Organização, e, simultaneamente, permita a defesa em profundidade e o apoio mutuo entre controlos, através da interligação entre os controlos tecnológicos, os procedimentos / processos e as boas práticas dos utilizadores, em múltiplas camadas de proteção.

A gestão operacional passa por, eventualmente, implementar um *Security Operations Center (SOC)*, com a capacidade mínima para auditar e monitorizar os controlos de Cibersegurança implementados, alguns dos quais associados, também, à Segurança da Informação e certamente à proteção de dados pessoais.

Por outro lado, é importante perceber e aceitar que o incidente vai ocorrer, consequentemente, há necessidade de desenvolver a capacidade de ***Resposta a Incidentes e Recuperação de Desastres***, no mínimo, com planos de contingência operacionais e treinados para a gestão de incidentes e a recuperação de desastres de TI. Será, possivelmente, necessária na execução de algumas ações, a colaboração (e partilha de informação) de entidades externas à Organização (e.g., ISP, Centro de Cibersegurança Nacional, Policia de Investigação Criminal).

É claro que a Organização, numa abordagem holística deve considerar todos os aspetos de segurança no seu plano de ***Continuidade de Negócio***, garantindo que tem capacidade para continuar a entregar produtos ou serviços aos clientes nos níveis acordados e aceitáveis após um incidente.

Tabela 5: Gestão Operacional

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Liderança Digital	Equipas Virtuais	(Ford, Piccolo e Ford, 2017); (Chang, Hung, Hsieh, 2014)
Monitorização e Auditorias	Ferramentas *Open Source* (e.g., GLPI, Nagios); SIEM	(Liska, 2015); (Jacobs e Rudis, 2014); (ISO 19011, 2012)
Gestão de TI	ISO 20000-1, ITIL	(Turban, Rainer e Potter, 2003); (ISO 20001, 2015); (ITIL 3, 2007)
Framework de **Controlos de Segurança**	Dimensões, Categorias e Controlos; Funcionalidades de um CSIRT	Martins, Santos, Nunes e Silva (2012a);

		Martins, Santos, Rosinha and Valente (2013); (Martins, 2015); (SANS, 2013)
Resposta a Incidentes e Recuperação de Desastre	Processo e Ferramenta de Gestão de Incidentes; Plano de *Disaster Recovery*	(Whitman, Mattord e Green, 2014); (NIST 800-34, 2010); (NIST 800-61, 2012); (ISO 27035, 2011)
Continuidade de Negócios e Gestão de Crises	Plano de Continuidade de Negócio	(Whitman, Mattord e Green, 2014); (ISO 22301, 2012); (BCI, 2013)

Nas dimensões anteriormente descritas existe uma variável cuja *"Parametrização e Controlo"* é quase impossível numa arquitetura de Segurança da Informação e Cibersegurança e que é o "Elemento Humano". A sua manipulação, através de ataques de Engenharia Social, pode pôr em causa todo o processo de segurança ou a tecnologia implementada na Organização, consequentemente, este elemento necessita de formação, sensibilização e treino ajustado a uma realidade complexa e em permanente mudança.

7.A FORMAÇÃO, SENSIBILIZAÇÃO E TREINO

Tal como afirma PELTIER, um programa eficaz de Segurança da Informação não pode ser implementado sem promover um programa de treino e consciencialização dos colaboradores, o qual deve endereçar políticas, procedimentos e ferramentas (2005).

Nesta dimensão é fundamental: (i) utilizar técnicas corretas de ensino na transmissão de conhecimento, através de ações de formação, sensibilização e treino, presenciais ou *online*; (ii) analisar as competências necessárias dos colaboradores nos diferentes níveis da Organização; (iii) desenvolver conteúdos pedagógicos apelativos; (iv) utilizar plataformas de *E / B-learning* para disponibilizar os conteúdos; (v) realizar exercícios coletivos e treino individual; (vi) e por fim, garantir uma gestão de conhecimento focada na gestão das lições apreendidas com incidentes de segurança (Figura 7).

Um aspeto nuclear, é aplicar na formação, sensibilização e treino dos colaboradores, as mais recentes ***Técnicas de Ensino*** (e.g., jogos, ambientes de simulação) ajustadas às audiências e em função das suas necessidades (competências a obter – "*To Be*"). Pressupõe-se, consequentemente, uma prévia identificação das ***Competências dos Colaboradores*** nas temáticas de Segurança da Informação e Cibersegurança ("*As Is*"), bem como a integração destas nas descrições de funções do colaborador e no plano de formação anual da Organização.

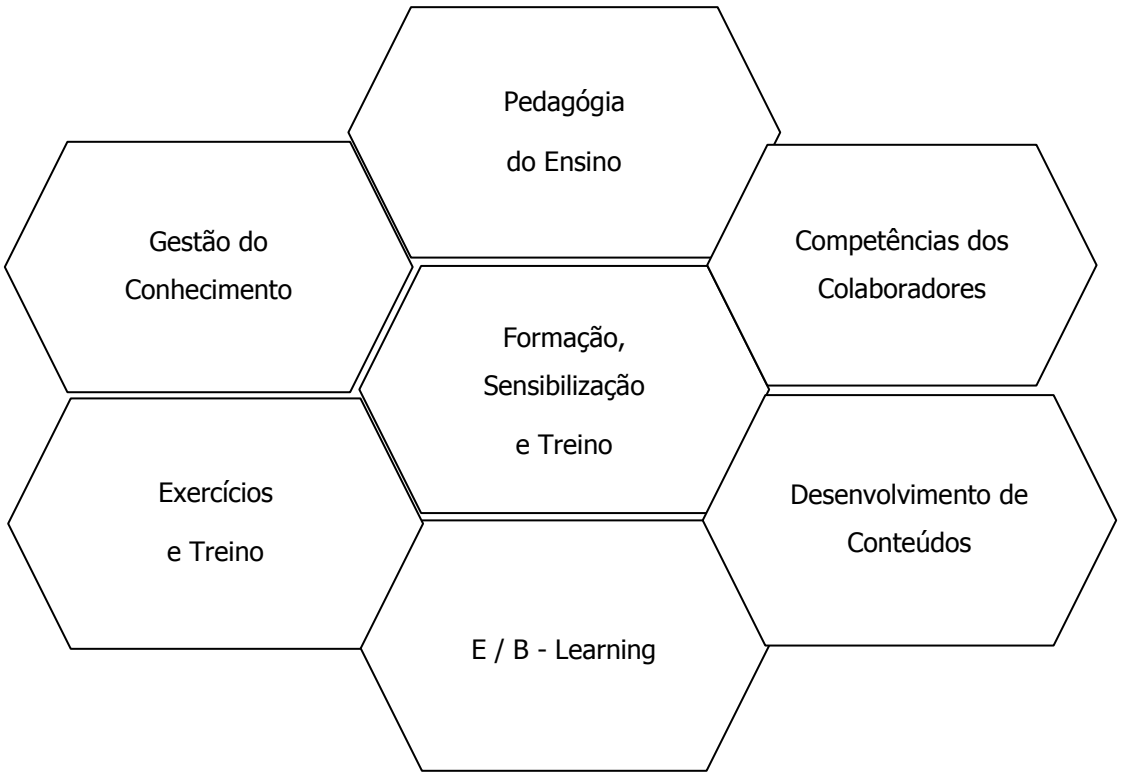

Figura 7: Formação, Sensibilização e Treino

É necessário, também, ***Desenvolver Conteúdos*** para as ações de formação e sensibilização (e.g., jogos), que permitam maior realismo, intervenção dos colaboradores da Organização e que facilitem a "passagem da mensagem", disponibilizando os conteúdos, sempre que possível, através de ***Plataformas de E-learning*** (e.g., *Moodle*), pelas vantagens que daí resultam.

Algumas das possíveis abordagens passam pela realização de ***Exercícios*** e ***Treino*** dos colaboradores (e.g., reagir a um ataque de *phishing*), pela realização de laboratórios em ambientes de simulação (e.g., *Cross Site Scripting*) ou a participação em exercícios coletivos (e.g., gestão de crises, recolha de informação de fontes abertas - OSINT).

Outro aspeto nuclear é a partilha de experiências, de lições aprendidas entre os colaboradores da Organização. Uma das formas, entre outras, para realizar esta partilha é possuir um processo automatizado para gestão de incidentes (e de problemas), que possibilite disponibilizar *Casos de Estudo* aos que necessitam de os conhecer em função das suas atividades e cujo objetivo principal é evitar a repetição de erros. Garante-se deste modo a ***Gestão de Conhecimento*** na área da Segurança da Informação

Nesta dimensão, existe, também, um conjunto de MTF (Tabela 6), cuja indicação neste artigo resulta da sua aplicação pelos autores em diversas atividades de ensino, de treino militar e ainda em formação certificada.

Tabela 6: Formação, Sensibilização e Treino

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Pedagogia do Ensino	Técnicas de Ensino (e.g., Casos de Estudo)	(Sternberg, Sternberg e Mio, 2012); (Jensen, 2009); (MTP, 2003)

Análise de Competências	Manual de Funções da Organização; Plano Anual de Formação	(NIST 800-118, 2017); (NIST 800-16, 2014); (Peltier, 2005); (Siponen, 2001); (Mann, 2008); (Hadnagy, 2011)
Desenvolvimento de Conteúdos	Jogos de Guerra	(Creveld, 2013); (Dunnigan, 2000); (Michael e Chen, 2005)
Plataformas de E - Learning	Ensino *online*	(PROLEARN, 2004); (Nash, Susan and Moore, 2014)
Exercícios e Treino	Laboratórios de Simulação, Exercícios (e.g., Gestão de Crises*)*	(ENISA_ Training, 2014); (NIST 800-50, 2003); (Martins et al., 2016)
Gestão do Conhecimento	Modelos de Gestão do Conhecimento	(Nonaka e Takeuchi, 1995); (PDE_0-32-00, 2012)

Embora todas as Dimensões / Sub-dimensões referenciadas anteriormente sejam fundamentais para o desenho e a implementação de uma eficaz Arquitetura de Segurança da Informação e Cibersegurança, é necessário que esta integre a

formação, sensibilização e o treino nestes domínios de todos os colaboradores da Organização.

8.CONSIDERAÇÕES FINAIS

Este artigo propõe um modelo que identifica e interliga algumas das mais importantes, senão a maioria das atividades necessárias para a implementação de um Sistema de Gestão de Segurança da Informação, que simultaneamente considera a Cibersegurança e a Proteção de Dados Pessoais. Modelo este, orientado para a atividade profissional dos CISO, dos Encarregados de Proteção de Dados, dos Consultores e Gestores de Projetos que procuram possuir uma visão holística destas temáticas. O modelo proposto é suportado numa revisão de literatura, na experiência dos autores obtida durante a sua atividade académica, em auditorias e implementação de Sistemas de Gestão de Segurança da Informação e em projetos de *desenho* e implementação de Sistemas de Informação.

Como principais resultados obtidos deste estudo, salientam-se: (i) o modelo para a gestão de Segurança da Informação, Cibersegurança e Proteção de Dados; (ii) e a identificação e sugestão de um possível conjunto de competências profissionais, necessárias para a atividade profissional dos responsáveis pela Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais.

Conclui-se ainda que a gestão da Segurança da Informação, a Cibersegurança e a Proteção de Dados Pessoais nas organizações possuem um conjunto de atividades comuns, que, direta ou indiretamente, contribuem para garantir as propriedades fundamentais de Segurança da Informação.

A principal limitação do modelo proposto passa por apenas descrever, sumariamente, as dimensões / Sub-dimensões, os métodos e as técnicas, e não identificar as interligações entre as Sub-dimensões deste. No entanto, isso deve-se ao facto de se tratar de um trabalho em progresso, onde futuramente *se* procurará que o modelo proposto seja validado através da aplicação de um *questionário* a

especialistas nestas temáticas e do método de investigação *Action Research* aplicado a projetos de implementação de SGSI, Cibersegurança ou Proteção de Dados Pessoais.

Os trabalhos futuros passarão por "desdobrar" o modelo proposto num método de implementação de um SGSI, que inclua a identificação e descrição das principais capacidades operacionais e de apoio.

A abordagem destas temáticas necessita de uma visão integrada, multidisciplinar, sistemática e da dedicação de verdadeiros especialistas em permanência nas Organizações.

Agradecimentos

Um agradecimento especial ao Pessoa Dinis e ao João Bessa Pacheco pelas sugestões de simplificação do artigo para uma mais compreensível leitura por leitores não especialistas. Ao João, especialmente pelo contraditório que obrigaram à reflexão e clarificação de alguns dos conceitos e ao Dinis pela discussão sobre a temática da gestão de equipas virtuais.