

# SUBSÍDIOS PARA UMA EFICAZ SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

*José Carlos Lourenço Martins* <sup>(\*)</sup>

*TCOR INF (Eng.º)*

*Henrique Manuel Dinis dos Santos* <sup>(\*\*)</sup>

*Professor Doutor*

*Paulo Viegas Nunes* <sup>(\*\*\*)</sup>

*TCOR TM (Eng.º)*

## RESUMO

Nas organizações, a informação é um dos activos mais importantes, suportando todos os seus processos de negócio com fins lucrativos ou não, devendo garantir permanentemente a continuidade do negócio, sem alteração de algumas das propriedades fundamentais da informação: confidencialidade, integridade e disponibilidade.

Os Sistemas de Informação ao procurar satisfazer as necessidades de informação dos processos de negócio, são um dos factores determinantes para a competitividade das organizações, constituindo uma ferramenta que estimula a sua produtividade, imprescindível ao processo de tomada de decisão aos vários níveis de gestão.

No entanto as organizações actualmente integradas numa sociedade em rede através da Internet, devem preparar-se para novas ameaças dirigidas aos seus

---

<sup>(\*)</sup> Professor da unidade curricular de Introdução à Programação e Bases de Dados na Academia Militar e da Pós-Graduação em Guerra de Informação/Competitive Intelligence. Mestre em Sistemas de Informação pela Universidade do Minho.

<sup>(\*\*)</sup> Docente e investigador na área disciplinar de Sistemas de Computação e Comunicações, do Departamento de Sistemas de Informação, da Escola de Engenharia, da Universidade do Minho. Coordenador do Centro de Investigação Algoritmi, da Universidade do Minho. Professor da Pós-Graduação em Guerra de Informação/Competitive Intelligence.

<sup>(\*\*\*)</sup> Coordenador científico e Professor da Pós-Graduação em Guerra de Informação/Competitive Intelligence. É membro do CINAMIL – Centro de Investigação da Academia Militar.

Sistemas de Informação organizacionais, independentemente do tipo de organização, da dimensão, da natureza (pública ou privada) e dos recursos de tecnologias de informação e comunicação existentes.

Este artigo permite lançar alguns pontos de reflexão sobre a temática da Segurança da Informação, numa perspectiva integradora e global. Pretende fundamentalmente apresentar de forma didáctica e simplista uma visão sistémica de possíveis dimensões e componentes a considerar para a eficaz Segurança da Informação.

**Palavras-Chave:** Gestão da Segurança da Informação, Sistemas de Informação, Identificação e Avaliação do Risco.

## INTRODUÇÃO

As organizações como "entidades complexas" integradas numa sociedade em rede, na sua maioria funcionam com base em processos formais ou *ad-hoc*, apoiados em fluxos de informação, manuseados por pessoas e suportados numa infraestrutura tecnológica ligada à Internet. Estas exigem uma eficaz segurança da informação, baseada numa análise rigorosa dos sistemas que interagem com as organizações, de forma a identificar as ameaças a que está sujeita.

Para proteger uma organização das ameaças à segurança dos seus recursos de informação ou da que está sob a sua responsabilidade, deve a organização possuir uma política de segurança. Esta constitui um documento aprovado pela gestão de topo, cujo objectivo principal é fornecer as directivas essenciais para a gestão da segurança da informação em toda a organização.

Para a definir, existe a necessidade de uma metodologia operacional de identificação e avaliação de riscos, que garanta fundamentalmente a segurança da informação. Na sua fase inicial é necessário definir a informação a ser protegida, identificando essencialmente os recursos que a suportam, as suas vulnerabilidades e as ameaças às quais está sujeita, determinando o seu impacto e probabilidade de realização de ataques associados.

A identificação e avaliação de riscos como processo dinâmico, deverá ser conduzido periodicamente, de forma a manter actualizados os vários indicadores de uma possível *Framework* de Segurança <sup>1</sup> que deve reflectir alterações externas e internas à organização, tendo sempre como objectivo principal, a segurança da informação.

Um dos seus aspectos principais, deverá ser a identificação dos riscos informáticos, em que, como refere Moreau (2003, p.170), é necessário considerar os "[...] *riscos relativos aos processos operacionais induzidos pelo Sistema de Informação e, por outro, os riscos inerentes à função informática (organização, recursos humanos, tecnologias informáticas e materiais, formas de gestão e funcionamento)*".

---

<sup>1</sup> No desenvolvimento de software uma *Framework* é uma estrutura de suporte, com vários componentes, com base na qual outro projecto de software pode ser organizado e desenvolvido. Uma *Framework* ajuda a desenvolver e juntar diferentes componentes num projecto de software. *Frameworks* são projectadas, com a intenção de facilitar o desenvolvimento de software, evitando que analistas e programadores gastem tempo com detalhes de baixo nível do sistema ou repetitivos. O mesmo conceito pode associar-se à Segurança da Informação.

Esta é uma situação complexa, na qual e a fim de construir soluções de segurança equilibradas e aceitáveis pelos diferentes intervenientes, temos que explicitar os critérios para a tomada de decisão na implementação de controlos, tendo em consideração as suas prováveis dimensões de segurança.

Os decisores têm que ter uma visão prospectiva, que lhes possibilite identificar os factores que a curto e a médio prazo possam alterar a segurança dos Sistemas de Informação (SI) e conseqüentemente a segurança da informação. É necessário dispor de indicadores consistentes e realistas para minimizar as possíveis acções de Guerra de Informação / *Competitive Intelligence* sobre os SI.

Este artigo encontra-se dividido em seis secções, reflectindo uma abordagem onde se procurou privilegiar a simplicidade dos conceitos e promover a sua integração. Na primeira secção, efectua-se o enquadramento da Organização no "Ambiente Geral e de Tarefa" e apresentamos os níveis e actividades a que o Sistema de Informação terá necessariamente que dar resposta. Procuramos na secção dois, apresentar alguns dos modelos possíveis para a gestão da segurança da informação e abordar sumariamente a actividade de identificação e avaliação do risco. Em qualquer metodologia de análise de risco há que determinar ou estimar o valor da informação existente, o que efectuaremos na secção três, pela apresentação de um possível modelo. Na secção quatro, identificamos e analisamos possíveis métodos de ataque a que um Sistema de Informação poderá ser sujeito, focando na temática da Cibersegurança. De seguida, na secção cinco, são identificadas algumas das dimensões de segurança da informação mais relevantes na nossa opinião. Como corolário, são apresentadas as conclusões e possibilidades futuras de estudos.

## 1. AS ORGANIZAÇÕES E OS SISTEMAS ENVOLVENTES

Para uma eficaz segurança da informação é necessário uma análise dos sistemas que interagem com as organizações e dos diversos actores e suas relações, de forma a identificar e perspectivar as ameaças a que está sujeita. Um dos principais sistemas a analisar é a infra-estrutura crítica de apoio à organização, especialmente os subsistemas de energia eléctrica e telecomunicações.

Conforme refere o Tenente-General Jesus Bispo citado por Balsinhas (2003, p. 16), *"Infra-estrutura crítica é aquela cuja ruptura pode produzir efeitos de âmbito nacional, ou regional, de tal forma que afecte o regular funcionamento*

*dos serviços da sociedade civil e das instituições nacionais, criando um problema de Segurança Nacional. Neste contexto, é considerada infra-estrutura crítica toda a que obedeça ao critério anterior, e que seja controlada através de um Sistema de Informação, para a regulação automática ou semi-automática do seu funcionamento".*

A identificação dos sistemas externos que interagem com a organização permite enquadrá-la no ambiente envolvente e obter uma visão real das ameaças à sua sobrevivência. Neste processo, é essencial possuir uma tipologia de ameaças e uma metodologia para a sua análise que permita posicionar as capacidades e intenções das ameaças para actuar sobre as vulnerabilidades dos activos críticos das organizações.

Após a análise externa das organizações, é necessário integrar a interna, o que passa fundamentalmente por referenciar as possíveis ameaças e vulnerabilidades dos componentes (num sentido lato, englobando todos os recursos tecnológicos e humanos) dos Sistemas de Informação.

### *NÍVEIS DE GESTÃO E ACTIVIDADES DE UMA ORGANIZAÇÃO*

Os Sistemas de Informação procuram satisfazer as necessidades de informação dos processos de negócio da organização, através de um conjunto de componentes inter-relacionados que reúnem ou procuram, processam, armazenam e distribuem informação destinada a suportar o processo de tomada de decisão e o controlo de uma organização (Laudon e Laudon, 2006), sendo um factor determinante para a competitividade das organizações e constituindo uma ferramenta imprescindível ao processo de tomada de decisão aos vários níveis de gestão. É fundamental analisar os diversos níveis e actividades da organização, identificando-se a informação existente em cada nível organizacional e os meios humanos e tecnológicos de suporte. Esta actividade gera um primeiro esboço dos fluxos de informação que percorrem as organizações, identificando-se os processos fundamentais onde esta é essencial para atingir os objectivos do negócio. Segundo a norma EN ISO 9001 (2000), um processo é qualquer actividade ou conjunto de actividades que utiliza recursos para transformar entradas em saídas. Uma análise exaustiva dos SI que suportam os níveis de gestão referenciados, vai permitir detalhar em profundidade as vulnerabilidades a que estão sujeitos e as medidas que estão implementadas ou planeadas para fazer face às vulnerabilidades da organização.

Nesta análise de vulnerabilidades terão que estar obrigatoriamente representadas as dimensões tecnológicas, física, humana (decisões constroem-se em termos de raciocínios individuais) e organizacional (processos de funcionamento). Esta fase consiste na essência em caracterizar internamente a estrutura e dinâmica da organização.

O critério que utilizamos para analisar e classificar os SI é o dos níveis de gestão suportados, segundo a Figura 1. A relevância desse critério é apontada por Amaral (1994, p. 48) ao afirmar que *"A importância da diferenciação dos diversos tipos de SI resulta do facto deles desempenharem papéis e terem utilidades distintas para a organização. Estas diferenças implicam atenção e tratamento diferenciado quando são envolvidos como objecto de atenção nas actividades de desenvolvimento, planeamento e gestão do SI global da organização"*.



Fonte: Adaptado de Laudon e Laudon (2006, p.41)

**Figura 1** - Níveis de uma Organização

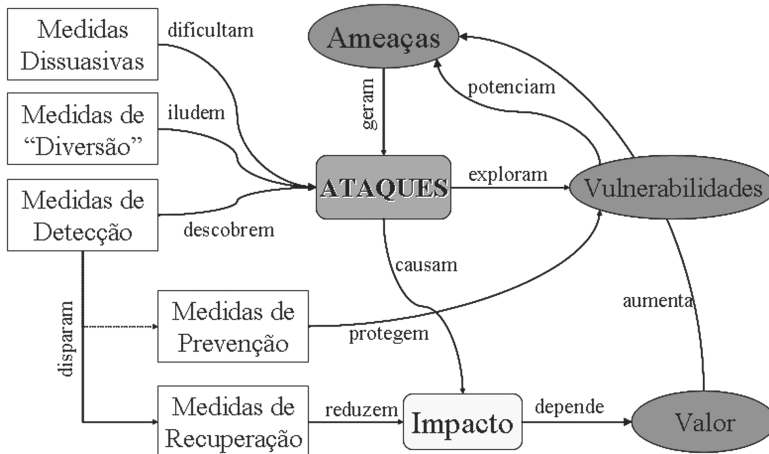
## 2. MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Para planear devidamente a segurança da informação, é importante dispor de um Modelo de Gestão da Segurança da Informação que garanta as propriedades fundamentais da segurança (no mínimo a confidencialidade, integridade e disponibilidade), permitindo planear devidamente a aplicação dos controlos de segurança relevantes.

Tal como refere Santos (2006, p. 1) *"[...] sem o adequado suporte de uma metodologia de gestão da segurança que aborde todo o processo de geração,*

processamento e armazenamento da informação, no contexto real da organização, dos seus objectivos e das suas práticas de trabalho, não é possível garantir um nível de segurança da informação adequado. E sem estes indicadores qualquer investimento em segurança pode ser sempre questionado".

Um possível modelo de suporte à segurança da informação é o apresentado na Figura 2, de simplificação conceptual e facilidade de integração com outras metodologias, onde a questão principal parece-nos ser a sua operacionalização.



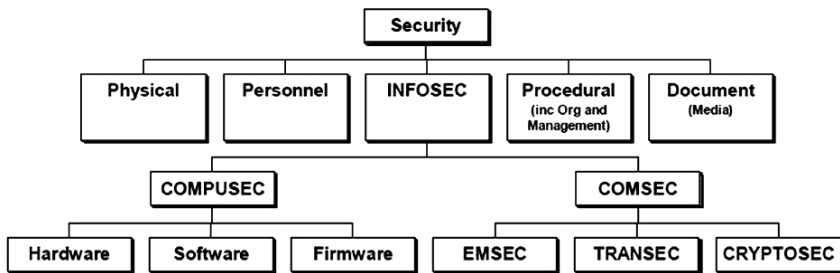
Fonte: Santos (2006, p.2)

**Figura 2 - Modelo de suporte à norma ISO / IEC 17799**

A aplicação deste modelo de segurança da informação, exige fundamentalmente a correcta identificação das ameaças, vulnerabilidades e a caracterização de ataques a que o recurso informação está sujeito, de forma a poder determinar o impacto de um eventual ataque. Essa análise permitirá construir uma Política de Segurança correcta, que defina todas as medidas necessárias a implementar para garantir a eficiente segurança da informação.

Tal como refere Santos (2008) um ataque é um conjunto de acções que, explorando uma ou mais vulnerabilidades do Sistema de Informação, violam as suas propriedades de segurança, provocando algum tipo de impacto nos recursos. Para os ataques conhecidos é possível actuar sobre as vulnerabilidades que são exploradas, bloqueando as ameaças que nelas têm origem.

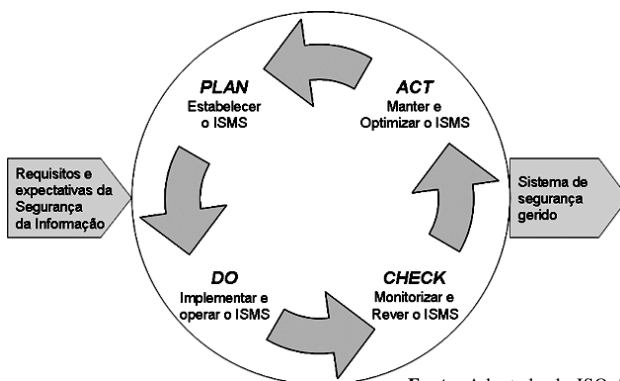
A NATO definiu um modelo que podemos observar na Figura 3, onde se realçam os seus elementos fundamentais de segurança. Este modelo separa as preocupações relacionadas com as comunicações e os computadores, definindo, superiormente, um conjunto de eixos que separam os objectos de análise.



Fonte: NATO <sup>2</sup>

Figura 3 - Modelo de Segurança da NATO

No entanto, qualquer dos modelos sugeridos ou futuramente desenvolvidos deve enquadrar-se com a utilização de um modelo de processo conhecido como PDCA (*Plan-Do-Check-Act*) de acordo com a norma ISO / IEC 27001 (2005), à semelhança do que é adoptado na norma ISO 9001 (2000), o qual se encontra ilustrado na Figura 4.



Fonte: Adaptado da ISO / IEC 27001 (2005)

Figura 4 - Modelo PDCA para um Sistema de Gestão de Segurança da Informação

<sup>2</sup> Site restrito da NATO (Versão 1.6 de 8 de Outubro de 2007).

No modelo PDCA é preconizado um ciclo de actividades que, no seu conjunto, define a forma de estabelecimento de um Sistema de Gestão da Segurança da Informação, que integra: a sua implementação e operação, a sua monitorização e revisão e, finalmente, a sua optimização em função dos resultados obtidos em cada iteração do processo (Santos, 2006).

### *IDENTIFICAÇÃO E AVALIAÇÃO DO RISCO DE SEGURANÇA*

Entre as várias actividades de Gestão da Segurança da Informação encontra-se a identificação e avaliação do risco de segurança. Esta assegura que uma organização identifica e modera a potencial perda de recursos em caso de desastres, possíveis interrupções de serviços em operações resultantes de acções humanas ou de outras origens tais como sabotagens, acções maliciosas perpetradas por empregados descontentes ou por negligência (Serrano e Jardim, 2007). Os gestores devem conhecer os factos que podem comprometer os objectivos de negócio e tomar decisões que permitem controlar os seus efeitos (Ferreira, 2001). Podemos referenciar diversas metodologias <sup>3</sup> para identificar e avaliar o risco de segurança, utilizadas em organizações militares e civis.

Ao nível das normas Internacionais podemos referenciar a título de exemplo a norma ISO/IEC TR 13335-3 (1998) e a BS 7799-3 (2006). A nível académico a metodologia OCTAVE (*Operationally Critical Threat, Assets, And Vulnerability Evaluation*), desenvolvida no *Software Engineering Institute da Carnegie Mellon University* preconiza um processo de sessões onde os colaboradores que trabalham na área analisada da organização definem os riscos, medidas de protecção e participam em sessões de formação (Alberts e Dorofee, 2001).

No Exército Português, conforme refere Rosa (2003, p.42), uma das áreas prioritárias para avaliar o risco é a da segurança dos sistemas informáticos, em parte "[...] devido à sua complexidade, conectividade global e dependência dos sistemas de pessoas de confiabilidade desconhecida", não existindo no entanto uma metodologia adoptada para o efeito, mas somente um conjunto de boas práticas de segurança, sem integração e sistematização na sua operacionalização.

---

<sup>3</sup> Descritos alguns modelos utilizados nas organizações militares por Rosa (2003) e alguns aplicados nas organizações civis em Ferreira (2001).

### 3. O PAPEL DA INFORMAÇÃO

Em qualquer metodologia de análise de risco há que determinar ou estimar o valor da informação existente, analisando as dimensões que afectam o seu valor e utilidade. Há algumas teorias que se podem aplicar nesta área, muitas delas inspiradas nas teorias económicas, como por exemplo a de Howard (1996) e de Hilton (1981). Outras há que se inspiram nos conceitos de Guerra da Informação, como a apresentada por Alberts et al. (1999) e Nunes (2005), que são as que seguiremos neste artigo.

Nesta abordagem, o valor da informação é determinado segundo as dimensões indicadas na Figura 5 (Qualidade, Temporalidade e Conteúdo). Estas dimensões são utilizadas procurando identificar a informação mais valiosa que permita obter uma posição de superioridade no domínio da informação em relação a um oponente, quer seja reduzindo a capacidade que o adversário tem de obter informação sobre a nossa organização (posição da informação "vermelha") quer seja procurando aumentar a nossa informação sobre o adversário (posição

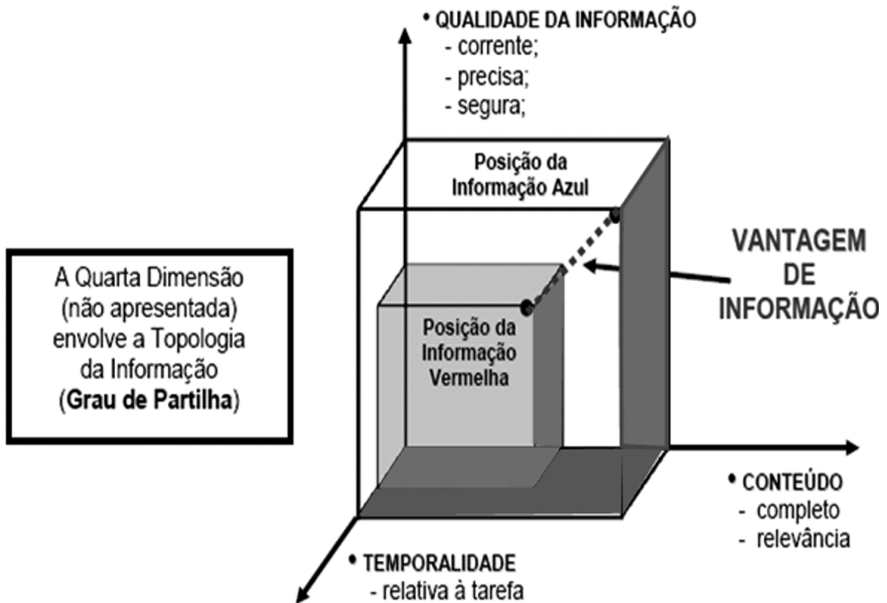
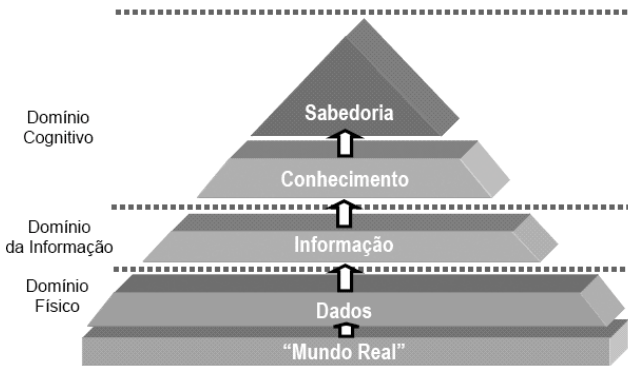


Figura 5 - Superioridade de Informação

da informação "azul"), garantindo a permanente segurança da informação. O objectivo a atingir pela organização "azul" será o de aumentar tanto quanto possível o diferencial existente no domínio da informação relativamente à organização "vermelha", convertendo depois essa assimetria numa vantagem operacional (Nunes, 2005).

Uma outra abordagem possível é a inspirada nos sistemas de Comando e Controlo (C2), que consideram os domínios ilustrados na Figura 6. Estes domínios permitem perspectivar prováveis "eixos e modalidades de ataques" que explorem as vulnerabilidades existentes nos domínios apresentados (Físico, de Informação e no Cognitivo).



Fonte: Adaptado do relatório final do grupo SAS-050 (2006, p.91)

**Figura 6 - Pirâmide Cognitiva**

Numa perspectiva Militar sobre estes domínios, suportada na descrição sintética de Nunes (2005), podemos indicar que o domínio físico é onde os nós dos sistemas de C2 e também as redes de comunicações que os interligam se situam. O domínio da informação é por excelência, o domínio onde a informação é estruturada, utilizada e partilhada e o domínio cognitivo traduz tudo aquilo que se passa na mente do decisor.

A visão militar de C2 tem por suporte os conceitos de Comando como a autoridade investida num indivíduo, para dirigir, coordenar e controlar uma Força militar e o Controlo definido como a autoridade exercida por um Comandante sobre parte das actividades das organizações subordinadas, ou outras organizações que estejam normalmente sob o seu comando, que engloba

a responsabilidade de implementar ordens e directivas (toda ou parte desta autoridade deve ser delegada).

Saliente-se que nesta área, a evolução tecnológica também fez evoluir este modelo, verificando-se que o C2 naturalmente conduziu ao C3I, adicionando as dimensões das Comunicações e das Informações e mais recentemente ao C4I (adicionando a dimensão dos computadores) que não é mais que um C3I suportado por Sistemas de Informação utilizando novas tecnologias.

#### 4. GUERRA DE INFORMAÇÃO / COMPETITIVE INTELLIGENCE

Para garantir a segurança da informação temos que identificar e analisar os possíveis métodos de ataque a que um SI poderá ser sujeito. Podemos observar, com base num dos possíveis modelos das Operações de Informação (OI) que seguiremos neste artigo, as possíveis acções que podem ser aplicadas aos vários níveis do Sistema de Informação (Figura 7).

Na análise deste modelo são perceptíveis os alvos a explorar pelos eventuais ataques, para produzir efeitos directa ou indirectamente nos níveis físico, da informação e no cognitivo. Devemos consequentemente procurar anular ou minimizar os seus efeitos através da implementação de um adequado conjunto de controlos (ex. políticas, procedimentos e tecnologia).

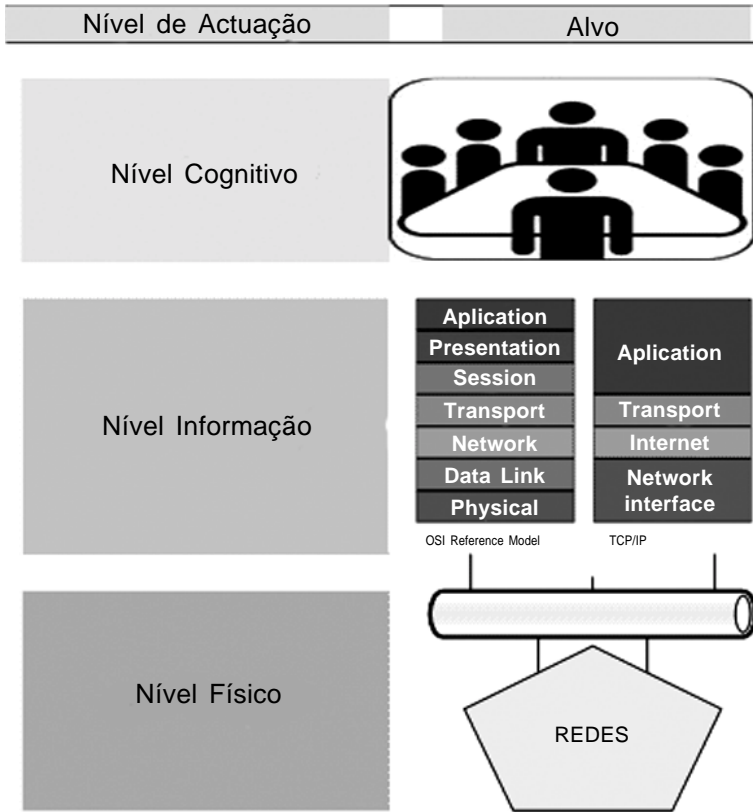
As acções ou possíveis métodos de ataque a que os SI poderão ser sujeitos, estão enquadrados dentro das Operações de Informação e consistem num conjunto de actividades e capacidades utilizadas para afectar a informação do adversário e os seus Sistemas de Informação (FM 100-06, 1996).

No contexto da Guerra da Informação, estas acções são desenvolvidas para obter a Superioridade de Informação, que consiste em obter uma vantagem operacional derivada da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega ao adversário essa mesma capacidade (FM 3-13, 2003).

No seio da NATO, com vista a promover um entendimento comum relativo às Operações de Informação, foi criado o grupo de trabalho RTG SAS-057<sup>4</sup> que

---

<sup>4</sup> *Research and Technology Group, do System Analysis and Studies Panel (SAS-057)*, que analisou doutrinas, políticas, conceitos, *Whitepapers*, publicados desde 1996.



Fonte: Adaptado do Modelo Operacional das OI segundo Waltz (1998, p.149)

**Figura 7** - Modelo Operacional das Operações de Informação

analisou documentação de diferentes Países / Organizações (Bélgica, Canada, Alemanha, Holanda, Noruega, Suécia, Reino Unido, Estados Unidos da América, OTAN, União Europeia, MNIOE <sup>5</sup>), tendo elaborado o seu relatório final em Outubro de 2006.

<sup>5</sup> *Multinational Information Operations Experiment*, liderado pela Alemanha, inclui a participação de Austrália, Canada, França, Reino Unido e Estados Unidos da América, para além da participação de outras nações tais como Bélgica, Portugal e Suécia.

A Divisão de Comunicações e Sistemas de Informação do Estado-Maior do Exército Português sintetizou as principais conclusões deste relatório e os principais conceitos doutrinários dos Estados Unidos da América e da NATO utilizados nas Operações de Informação e que apresentamos (DCSI/EME, 2007, p. 14):

- as Operações de Informação são actividades conduzidas no domínio da informação, para afectar a informação e os Sistemas de Informação com vista a atingir os efeitos desejados na vontade e capacidades adversárias e outras actividades desenvolvidas em apoio da concretização dos objectivos da missão enquanto se mantêm protegidos a informação e Sistemas de Informação das nossas Forças;
- existe uma lista de capacidades disponíveis <sup>6</sup> e actividades relacionadas, que podem ser aplicadas para a obtenção directa ou indirecta dos efeitos pretendidos com as Operações de Informação e que são fundamentalmente actividades:
  - de Influência, apresentando como alvo os decisores e elementos de entidades adversárias, bem como a população presente no Teatro de Operações, com vista a modificar comportamentos;
  - Anti-Comando, dirigidas à infra-estrutura de C4I de potenciais entidades adversárias;
  - de Informação, com vista a obter informações necessárias ao planeamento e execução de Operações de Informação e a proteger os decisores e as capacidades das nossas Forças;
  - Relacionadas, fundamentalmente através da coordenação e cooperação civil-militar e pela informação pública.

No conjunto das Operações de Informação, o contributo militar passa pela Guerra de Comando e Controlo (C2W), que consiste na utilização integrada de todas as capacidades militares, incluindo a Segurança das Operações, a Decepção, as Operações Psicológicas, a Destruição Física, a Guerra Electrónica e mais recentemente as *Computer Network Operations* (CNO), complementadas pelas actividades de protecção das Comunicações e dos Sistemas de Informação, com a finalidade de negar informação ao adversário. Em síntese, o objectivo é influenciar, degradar ou destruir as suas capacidades de C2, enquanto protegemos as nossas capacidades de comando e controlo contra acções similares (JP 3-13-1,1996).

---

<sup>6</sup> Tendo em consideração as funções das Operações de Informação no sentido de influenciar a própria vontade (de forças adversárias ou neutrais), afectar as capacidades que influenciam a vontade e a protecção contra as acções adversárias para influenciar a nossa vontade.

Considerando que actualmente a maioria dos métodos de ataques são executados usando as redes informáticas (Hildreth, 2001 e Richardson, 2008), ligadas através da rede das redes ou seja da Internet, é essencial a análise e compreensão do seu funcionamento.

### *CIBERSEGURANÇA*

A Internet como suporte tecnológico da sociedade em rede provoca alterações de poder, em virtude de suportar o ciberterrorismo, a cibercriminalidade e a *cyberwarfare* (Hildreth, 2001). Consequentemente a exploração da Internet exige uma atitude responsável por parte dos Estados, das Organizações e dos próprios Indivíduos, sob pena de as novas ameaças explorarem vulnerabilidades deste meio aberto de interacção e poderem pôr em risco a própria Segurança e Defesa Nacional (Martins e Nunes, 2008).

Segundo a UNESCO, o ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transacções económicas. É constituído por pessoas de todos os países, de todas as culturas e línguas, de todas as idades e profissões fornecendo e requisitando informação, de uma rede mundial de computadores interligada pela infra-estrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente (Balsinhas, 2003).

O Ciberespaço possibilita ataques planeados contra Sistemas de Informação via Internet, podendo consequentemente provocar incidentes graves, motivados pela destruição dos sistemas informáticos. Referimos a título de exemplo os SI dos Bancos ou das Bolsas (interrupção das transacções financeiras), dos Sistemas de Controlo Aéreo nos aeroportos (risco de colisão), dos Serviços de Emergência, da Sinalização das grandes cidades (paralisando o trânsito), entre outros.

Utilizamos neste artigo o termo "Rede de Computadores", quando falamos de um conjunto de computadores autónomos e interconectados (Tanenbaun, 1997), ou seja quando podem trocar informação.

Numa rede os utilizadores devem autenticar-se numa máquina, submeter explicitamente as tarefas remotas e explicitamente movimentar os ficheiros. No caso de uma *Local Area Network* (LAN), o cabo e os computadores formam a rede de suporte ao SI organizacional. O modelo considerado é o modelo Cliente/Servidor, no qual a comunicação é efectuada através de uma "mensagem de solicitação" do cliente enviada para o servidor e de seguida, este executa a tarefa e envia a resposta ao cliente.

Não existe uma taxonomia unanimemente aceite segundo a qual as redes de computadores se podem classificar, mas no entanto duas dimensões se destacam das demais: a escala e a tecnologia de transmissão (Tanenbaun, 1997).

Consideramos na essência as redes de difusão, que apenas têm um canal de comunicação, compartilhado por todas as máquinas e quanto à classificação por escala, as chamadas Redes Locais (LAN). As Redes Locais têm três características que as diferenciam das demais: o seu tamanho (normalmente de 10m a 1Km), a sua tecnologia de transmissão, que quase sempre consiste num cabo ao qual todos os computadores são conectados e a topologia. As LAN de difusão aceitam diversas topologias, mas para efeitos de modelo conceptual aplicado consideramos o padrão IEEE 802.3, mais conhecido por Ethernet™.

A um conjunto de redes interconectadas através de equipamentos (ex. routers), designamos de ligação inter-redes<sup>7</sup> ou apenas de inter-rede (Tanenbaun, 1997). A maioria das arquitecturas de redes foi organizada numa série de camadas ou níveis, em que o objectivo de cada nível é fornecer serviços ou seja um conjunto de primitivas (operações) para a camada acima dela. As entidades ao nível das camadas utilizam protocolos, que dizem respeito à implementação do serviço. O modelo de arquitectura que consideramos é o suportado no protocolo *Transmission Control Protocol - Internet Protocol* (TCP - IP), utilizado para funcionamento da Internet.

Face às anteriores considerações teóricas só perante uma "[...] *lista exaustiva das ameaças e da forma de as materializar em ataques ao sistema, é possível definir claramente a política de segurança e os meios de protecção necessários*" (Marques e Guedes, 1998, p. 244).

Indicamos alguns dos métodos de ataque mais focados em tecnologia (projectão de software malicioso e ataque a redes de computadores), de acordo com a classificação proposta por Kurose e Ross (2008) e que consiste na seguinte taxonomia: a utilização de *Malware* (ex. *Virus, worms e trojans*), o *Denial of service* (DoS), *Packet Sniffer*, *Masquerade* (ex. *IP spoofing*) e o modificar e apagar mensagens (*man-in-the-middle*).

Os efeitos de alguns destes métodos de ataque podem ser identificados no Ciberataque lançado contra a Estónia em Abril e Maio de 2007, durante o qual foram paralisadas praticamente todas as actividades do Estado.

---

<sup>7</sup> Um exemplo comum é um conjunto de LAN's conectadas por uma Wide Area Network (WAN).

Numa abordagem simplista podemos considerar que os ataques às redes de computadores desenvolvem-se em quatro fases (Tipton and Krause, 2004; Young and Aitel, 2004; Santos, 2008). Numa primeira fase (Levantamento: *Profiling*) procura-se identificar / localizar a (s) rede (s) da organização a atingir, após o que se verifica numa segunda fase, quais os computadores e serviços activos e, vulnerabilidades existentes (Pesquisa: *Scanning*). A terceira fase (Enumeração: *Enumeration*) tem como objectivo apoderar-se de contas de utilizador ou de direito de acesso a partilhas em máquinas da rede (entre outras) e por fim na fase quatro (Exploração: *Exploiting*), pretende-se fundamentalmente alterar a disponibilidade, confidencialidade ou a integridade da informação a que se teve acesso. As duas primeiras fases coincidem com uma possível metodologia de avaliação de segurança de redes (McNab, 2004 e Clarke e Nitesh, 2005).

É fundamental, considerar nesta temática da Segurança da Informação, as principais Tecnologias de Segurança implementadas ou a implementar e que passaremos a descrever sumariamente:

- os *Routers* como dispositivos que contribuem para a "defesa em profundidade", sendo a primeira tecnologia de segurança da rede de fora para dentro e o último de dentro para fora. Podemos utilizar como "filtro de pacotes", para análise dos fluxos de tráfego, permitindo maior rapidez que outros tipos de *firewalls* (com estado ou *proxy*). Podemos em termos militares entender os *routers* como as primeiras unidades a entrar em contacto com o inimigo; e se o inimigo entrar?
- as *Firewalls*, que são dispositivos por *hardware* ou *software* que possuem um conjunto de regras especificando que tipo de tráfego é permitido entrar ou sair da rede, diminuindo conseqüentemente a possibilidade de entrada de software malicioso e reduzindo a probabilidade de perturbações no funcionamento da rede. Permitem diferentes análises consoante o seu tipo (ex. filtragem automática, com estado ou *proxy*). A sua configuração terá sempre por base a política de segurança da organização, integrada com a identificação e avaliação de riscos efectuada. Podendo esta ser entendida como a primeira posição defensiva fortificada. As *firewalls* devem estar integradas se possível com os *Intrusion Detection System (IDS)*;
- os *IDS* funcionam como um sistema instalado na rede que detecta e alerta no caso de um evento anormal, devendo se possível estar integrados com as *firewalls*. Existem dois tipos de *IDS*, os baseados na rede (*NIDS*) e os

baseados nos *hosts* (HIDS). A sua finalidade principal é "olhar" para os dados em trânsito. Em termos militares podemos verificar que funcionam como os sistemas de sensores de uma posição defensiva;

- o Anti-vírus pretende detectar e remover código malicioso no sistema de ficheiros, sendo crítica a sua actualização automática e o *scanning dos hosts* (ex. *file servers, mail server e workstations*);
- as Virtual Private Network (VPN) são dispositivos que permitem que um utilizador externo participe na rede interna como se estivesse conectado directamente a ela. No entanto devemos garantir que as "pontas da conexão" são seguras, pois se uma ameaça conseguir obter um canal seguro para a rede interna organizacional então obtém uma arma poderosa para afectar as propriedades da informação. Estes "canais" seguros são possíveis mediante a utilização da criptografia simétrica ou assimétrica;
- a Criptografia é uma técnica de segurança que no caso da comunicação através da rede, garante canais de comunicação seguros, evitando que a informação seja perceptível a quem não possuir uma chave que permita decifrá-la (Marques e Guedes, 1998). As técnicas de criptografia para implementar canais de comunicação seguros podem subdividir-se em dois grandes grupos, pela utilização de:
  - chave secreta ou criptografia simétrica, em que uma chave é partilhada exclusivamente pelos agentes que interagem sobre um canal;
  - chave pública ou criptografia assimétrica, em que existem duas chaves, uma conhecida publicamente e outra que deverá ser mantida secreta, que permitirão cifrar e decifrar a informação.Podemos em determinadas situações efectuar apenas a autenticação da informação e deste modo garantir que o destinatário possa provar que o documento foi enviado por determinado agente. Sendo o uso da assinatura digital fundamental para assegurar a legitimidade da informação electrónica;
- *Honeypots* é uma tecnologia de segurança que permite iludir o atacante, ou seja, procura que este gaste os seus recursos, tempo e esforço, contra um sistema que na realidade "emula" um conjunto de serviços de rede, obtendo consequentemente informações sobre as suas acções e possibilitando que a organização se prepare cuidadosamente e aumente o seu conhecimento sobre a ameaça. Podemos por exemplo utilizando a virtualização (ex. VMware) simular uma rede inteira, utilizando apenas um único computador.

Nesta dimensão tecnológica é essencial a realização de testes de auditoria de forma a operacionalizar a defesa e obter métricas da eficiência dos controlos de segurança implementados. A título de exemplo e sem pretendermos ser exaustivos podemos referir os seguintes testes: *Network Scanning*, *Vulnerability Scanning*, *Password Cracking*, *Log Review*, *Integrity Checkers*, *Virus Detection*, *War Dialing*, *War Driving* (802.11 ou wireless LAN testing) e *Penetration Testing*. Em síntese, nas redes informáticas, é essencial garantir a segurança do perímetro, como limite fortificado da nossa rede e que pode incluir normalmente as tecnologias de segurança anteriormente apresentados (Northcutt et al., 2002). Também internamente deverão existir preocupações com a segurança da rede, que passam fundamentalmente, pelo uso de *firewalls* e anti-vírus nos clientes, no Sistema Operativo devidamente actualizado com os *patches* de segurança (e configurações correctas) e principalmente garantir-se as cópias de segurança da informação (incluindo dos computadores dos utilizadores).

## 5. DIMENSÕES DA SEGURANÇA

Uma organização em permanente evolução e adaptabilidade ao meio, necessita de identificar todas as suas vulnerabilidades, como características que potenciam o impacto da concretização de determinada ameaça referenciada.

Para a identificação e análise das dimensões de segurança de um SI, é necessária uma capacidade de percepção holística da segurança por parte dos seus responsáveis e não uma visão direccionada apenas para as Tecnologias de Informação (TI).

Um modelo conceptual para a Segurança da Informação exige a identificação, a gestão e o controlo dos diversos indicadores das dimensões da Segurança, facilitando a percepção da realidade da Segurança do SI pelos decisores. Devemos consequentemente identificar os principais componentes em que inserem os controlos de segurança.

A identificação dos prováveis componentes e indicadores para a segurança do SI deve ter por base duas abordagens distintas, com base em critérios de operacionalização e gestão. Numa abordagem *Top-Down* devemos referenciar os componentes principais de cada dimensão. Na realidade procuramos identificar as funções críticas e vitais para a organização, na perspectiva da segurança do SI e tendo como aspecto crítico garantir a continuidade do negócio da organização.

Paralelamente deve-se face à extensa literatura técnica existente sobre controlos a implementar para garantir a segurança da informação realizar uma abordagem *Bottom-Top*, em que procuramos agrupar os indicadores por funcionalidades de administração e semelhanças técnicas.

Na Segurança da Informação devemos numa primeira fase efectuar a análise da organização, da sua gestão, e do controlo de segurança do SI e da informação. Deve ser estabelecida uma estrutura de gestão para iniciar e controlar a implementação da Segurança da Informação dentro da organização. É fundamental a correcta visão geral da organização, de modo a garantir o correcto planeamento, implementação e a gestão de todos os controlos (indicadores) da Segurança da Informação. Para além da dimensão Tecnológica da Segurança da Informação, devemos ter preocupações com a dimensão da Segurança Física e a Humana (Erbschloe, 2005). Na Física procura-se garantir a protecção física dos SI no global e de todos os seus componentes (ex. hardware, software, documentação e meios magnéticos) no particular. A dimensão de Segurança Pessoal visa reduzir os riscos de erros humanos intencionais ou por negligência sobre os componentes dos SI, evitando principalmente os ataques de Engenharia Social, que vão explorar um dos elos mais fracos da segurança, o elemento humano.

Na Dimensão Tecnológica, devemos garantir o correcto processamento, transmissão e armazenagem dos dados e informação. Na rede, como conjunto de computadores autónomos e interconectados, existem como preocupações principais, a segurança das comunicações e a administração da rede com suporte aos sistemas operativos das tecnologias implementadas nos SI.

Nesta dimensão é fundamental ter em consideração a aquisição ou desenvolvimento, a implementação, manutenção e a correcta utilização do software instalado na organização (Pfleeger and Pfleeger, 2007 e Cannings et al., 2008), tendo especial atenção à separação dos ambientes de desenvolvimento, testes e produção de forma a impedir os riscos de segurança. Sendo também indispensável garantir o acesso autorizado dos utilizadores à informação e a sua correcta armazenagem e segurança.

## 6. CONSIDERAÇÕES FINAIS

A informação está exposta fundamentalmente a três elementos: a tecnologia, como componente que permite guardar, processar e transmitir a informação; as pessoas, ou seja todos os *stakeholders*, que podem aceder à informação,

através de redes privadas e da Internet e os processos de negócio utilizados na manipulação da informação (Solms e Posthumus, 2004).

Cada um destes elementos oferece um risco real para a segurança da informação, devendo ser preservada na essência as suas propriedades fundamentais, ou seja a confidencialidade, disponibilidade e a integridade (Solms e Posthumus, 2004; ISO / IEC 27001, 2005).

O risco associado à Segurança da Informação, é um componente de gestão de risco (Finne, 1998), para o qual temos várias opções de tratamento: aceitar o risco, evitá-lo, transferir ou mitigar (ISO / IEC 27001, 2005).

A decisão do nível de aceitação do risco pode ser baseada fundamentalmente nos critérios de nível de protecção da informação, nos factores de risco presentes ou na combinação dos dois e no retorno do investimento realizado após a implementação dos controlos de segurança da informação. A decisão de aceitação do risco em organizações militares, deve ter por premissa o garantir o nível mais elevado de segurança, em todas as dimensões da Segurança da Informação.

Para construir uma Framework de Segurança da Informação é necessário considerar os requisitos de segurança internos e externos (ex. aspectos legais e regulamentares), o que associado a um conjunto de boas práticas, permitirá uma correcta e eficiente Gestão da Segurança da Informação (Solms e Posthumus, 2004).

Devemos principalmente ter em consideração os componentes dos SI organizacionais. Estes usam fundamentalmente os computadores (*hardware e software*), as tecnologias para efectuar as comunicações (redes), com suporte em procedimentos organizacionais e nas pessoas que trabalham com o próprio sistema ou usam a sua saída (Turban et al., 2003).

As análises apresentadas permitem-nos reforçar a importância de identificar rigorosamente as ameaças, as vulnerabilidades e da necessidade de construir um modelo conceptual de Segurança da Informação que represente as Dimensões, Componentes e Indicadores a ter em consideração para operacionalizar um sistema integrado de segurança dos SI organizacionais (*Framework* de Segurança), que permita fornecer aos decisores um Modelo de Gestão da Segurança da Informação eficiente.

## REFERÊNCIAS BIBLIOGRÁFICAS

- ALBERTS, Christopher e DOROFEE, Audrey (2001). *OCTAVE – Method Implementation Guide Version 2.0*, Carnegie Mellon, Software Engineering Institute, United States of America.
- ALBERTS et al. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series, Washington, United States of America.
- AMARAL, L. (1994). *PRAXIS – Um Referencial para o Planeamento de Sistemas de Informação*, Tese de Doutoramento, Universidade do Minho, Guimarães.
- BALSINHAS, Paulo (2003). *Os Riscos do Ciberespaço – Análise e Gestão dos Riscos nas Infra-Estruturas Críticas de Informação*, Pós-Graduação em Guerra de Informação/Competitive Intelligence, Academia Militar, Lisboa.
- BS 7799-3 (2006). *Information Security – Managements Systems*, Part 3: Guidelines for Information Security Risk Management.
- CANNINGS et al. (2008). *Hacking Exposed Web 2.0*. Mc Graw Hill, United States of America.
- CLARKE, Justin and NITESH, Dhanjani (2005). *Network Security Tools*. O’Reilly, United States of America.
- DCSI/EME (2007). *Elemento de Guerra de Informação – Estrutura e Implicações*, MDN/Exército/EME, Lisboa.
- EN ISO 9001 (2000). *Sistemas de gestão da qualidade, requisitos*. Norma Portuguesa.
- ERBSCHLOE, Michael (2005). *Physical Security for IT*. Elsevier Digital Press, United States of America.
- FERREIRA, Rui (2001). *Gestão de Riscos de Sistemas de Informação*, Dissertação de Obtenção do Grau de Mestre em Gestão de Sistemas de Informação, ISCTE, Lisboa.
- FINNE, Thomas (1998). "A Conceptual Framework for Information Security Management", in *Vários, Computers & Security*, 17, p. 303-307.
- FM 100-06 (1996). *Information Operations*, Headquarters, Department of the Army, Washington, United States of America.

- FM 3-13 (2003). *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, Headquarters, Department of the Army, Washington, United States of America.
- HILDRETH, Steven (2001). *Cyberwarfare, Report for Congress U.S. Congressional Research Service*, the Library of Congress, United States of America.
- HILTON, Ronald W. (1981). "The Determinants of Information Value: Synthesizing Some General Results", in Vários, *Management Science*, Vol. 27, No. 1, p. 57-64.
- HOWARD, R.A. (1996). "Information Value Theory", in Vários, *Systems Science and Cybernetics – IEEE Transactions*, Volume 2, Issue 1, p. 22-26.
- ISO /IEC: 27001(2005). *Information technology – Security techniques – Information Security Management Systems – Requirements*.
- ISO/IEC TR 13335-3 (1998). *Information technology- Guidelines for the management of IT Security. Part 3: techniques for the management of IT security*.
- JP 3-13 (2006). *Joint Doctrine for Information Operation*, United States of America.
- JP 3-13.1 (1996). *Joint Doctrine for Command and Control Warfare*, United States of America.
- KUROSE, James e ROSS, Keith (2008). *Computer Networking*, Addison Wesley, 4<sup>th</sup> Edition, United States of America.
- LAUDON, Kenneth C. e LAUDON, Jane P. (2006). *Management Information Systems*, Prentice Hall, 9<sup>th</sup> Edition, United States of America.
- MARQUES, José e GUEDES, Paulo (1998). *Tecnologias de Sistemas distribuídos*. FCA - Editora de Informática, Lisboa.
- MARTINS, José Carlos L. e NUNES, Paulo Viegas (2008). " A Internet como factor de Transformação Social e das Relações de Poder", in Vários, *Proelium*, Revista da Academia Militar, VI Série, N.º 9, p. 135-158.
- McNAB, Chris (2004). *Network Security Assessment*. O'Reilly, United States of America.
- MOREAU, Frank (2003). *Compreender e Gerir os Riscos*, Bertrand Editora, Lisboa.
- NORTHCUTT, Stephen et al. (2002). *Segurança de Redes*, SANS GIAC, Editora Campus, Rio de Janeiro.
- NUNES, Paulo (2005). *O Impacto da Aplicação do Conceito de Network Centric Warfare nas Forças Armadas Portuguesas: Subsídios para o Levantamento de uma Capacidade Militar Centrada em Rede*, Lição Inaugural na Academia Militar, Lisboa.

- PFLEEGER, C. P. and PFLEEGER, S. L (2007). *Security in Computing*, Prentice Hall Professional Technical Reference, 4<sup>th</sup> Edition, United States of America.
- RICHARDSON, Robert (2008). *The 13<sup>th</sup> Annual Computer Crime and Security Survey*, Computer Security Institute, United States of America.
- ROSA, Manuel (2003). *Análise de Risco: Uma Ferramenta de Apoio à Decisão*, IESM, Lisboa.
- SANTOS, Henrique D. (2006). "ISO/IEC – A norma das normas em Segurança da Informação", in Vários, *Publicação da Associação Portuguesa para a Qualidade*, pp 11-1, Ano XXXV, N.º 1, Lisboa.
- SANTOS, Henrique (2008). *Apontamentos de Segurança Digital*, Pós-Graduação em Guerra de Informação/Competitive Intelligence, Academia Militar, Lisboa.
- SAS- 050 (2006). *Exploring New Command and Control Concepts and Capabilities*, Final Report – NATO.
- SERRANO, António e JARDIM, Nuno (2007). *Disaster Recovery – Um Paradigma na Gestão da Continuidade*, FCA – Editora de Informática, Lisboa.
- SOLMS, Rossouw Von e POSTHUMUS, Shaun (2004). "A framework for the governance of information security", in Vários, *Computers & Security*, 23, p. 638-646.
- TANENBAUM, Andrew (1997). *Redes de Computadores*, Editora Campus, 3.<sup>a</sup> Edição, Rio de Janeiro.
- TIPTON, F. Harold and KRAUSE, Micki (2004). *Information Security Management Handbook*. 5<sup>th</sup> Edition, Averbach, United States of America.
- TURBAN et al. (2003). *Administração de Tecnologia de Informação*, Editora Campus, Rio de Janeiro.
- YOUNG, Susan and AITEL, Dave (2004). *The Hacker's Handbook*. Averbach, United States of America.
- WALTZ, Edward (1998). *Information Warfare: Principles and Operations*, Artech House, United States of America.