Universidade do Minho

Academia Militar

FRAMEWORK DE SEGURANÇA DE UM SISTEMA DE INFORMAÇÃO

Dissertação apresentada como requisito parcial para obtenção do grau de

Mestre em Sistemas de Informação

ORIENTADORES

Prof. Dr. Henrique Manuel Dinis dos Santos
(Universidade do Minho)

TCor TM (Eng.º) Paulo Viegas Nunes
(Academia Militar)

SUBMETIDO POR

José Carlos Lourenço Martins

Lisboa
Julho de 2008

AGRADECIMENTOS

Aos meus orientadores pelas suas sugestões e incentivo na busca da excelência académica e que se na realidade não atingi, a eles certamente não se deve.

Ao Centro de Dados da Defesa pela possibilidade de validação da tese, com uma palavra de apreço e amizade ao responsável pela Divisão de Administração e Comunicações e Segurança, TCor Artª (Engº) António Galindro.

Ao Sr. Fernando Fevereiro Mendes por me ter possibilitado a consulta de documentação fundamental para a compreensão da temática da Segurança da Informação.

Aos meus pais António e Maria por me terem ensinado o valor da honestidade e do trabalho. E por último, mas nem por isso menos importante à Ana Bela, Inês e Guilherme pelo seu apoio, incentivo e amor.

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 são um factor determinante 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.

A actual sociedade em rede suportada fundamentalmente na Internet, apresenta novas ameaças dirigidas aos 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.

Dada a complexidade e abrangência da questão, existe a necessidade de uma *Framework* de Segurança, para garantir fundamentalmente a segurança dos recursos de informação, integrando diferentes visões: a da comunidade científica (modelo conceptual), a percepção dos decisores (modelo comportamental) e o modelo tecnológico de suporte aos processos de negócio.

Para proteger uma organização das ameaças à segurança da sua informação ou da que está sob a sua responsabilidade, deve a organização possuir uma política de segurança, sendo necessário simultaneamente uma identificação e avaliação de riscos.

É necessário, para a eficaz segurança da informação nas organizações, uma análise dos sistemas e actores que interagem com a organização, de forma a identificar actuais e futuras ameaças aos seus recursos e fluxos de informação. Esta análise permitirá apresentar uma visão macroscópica das ameaças que poderão surgir aos vários níveis de gestão das organizações, suportados por diversos Sistemas de Informação que, de forma contínua, procuram explorar as suas vulnerabilidades.

Propomos então apresentar uma *Framework* de Segurança para um Sistema de Informação, para garantir a segurança de um dos seus principais activos, a informação e servir como possível modelo de gestão de segurança da informação, aos decisores das organizações na tomada de decisões sobre a segurança da informação e sua gestão.

Procuraremos simultaneamente minimizar as possíveis acções de Guerra de Informação / Competitive Intelligence, reflectindo nesta *Framework* vários *Standards* de boas práticas da segurança da informação. Temos como objectivo principal garantir a protecção dos SI organizacionais dos métodos de ataque produzidos com base nas actuais ameaças e tipo de armas utilizadas (físicas, de sintaxe e semânticas).

A *Framework* de Segurança a obter deverá ser de fácil operacionalização nos diversos níveis de gestão organizacional, aberta a novas evoluções tecnológicas, suportar facilmente a reengenharia de processos, integrar metodologias internas da organização e de fácil leitura.

PALAVRAS – CHAVE: Guerra de Informação, Gestão da Segurança da Informação, Análise e Avaliação do Risco.

ABSTRACT

One of the most important elements in an organization is information, which supports all of the negotiation process with profitable ends (or not) that must try to guarantee at all times, if not permanently, information`s fundamental properties: confidentiality, integrity, and availability.

Information Systems are a determining factor for the organization's capacity, consisting of a tool that stimulates its productivity, indispensable in the deciding making process at the various levels of management.

The current network society supported primarily through the Internet, presents new threats to information networks that support organizational Information Systems, independent from the type of dimension, nature, organization, technological information resources, and existing communications.

Consequently it demands the utilization of a Security Framework in order to guarantee the security of information resources, integrated in a scientific community (conceptual model); decider's perception (behavioural model); and a technological model as support for negotiation processes.

An established security policy and operational identification and evaluation methodology of risk must be distinguished in order to protect an organization from threats to its information or information which it is responsible for.

It is necessary in order to guarantee information security efficiency, in an organization, an analysis of the system, and its agents that interact with the organization, in a way that could identify present and future threats to its resources and information fluxes. This analysis allows one to present a macroscopic vision of the threats that are in the various levels of management of the organization, supported by several Information Systems that, in a continuous form, search to discover its own vulnerabilities.

We propose to present a Security Framework for organizational Information Systems, to guarantee the security of one of the principle actives information and to serve as a possible model of security information management, to the deciders from the organizations in the choice making process on information security and management.

We search to minimize the possible actions of Information Warfare / Competitive Intelligence, outlining in this framework the various standards of good information security practise. We have as an objective to guarantee the protection of Information Organizational Systems from the various methods of attack produced by present day threats and types of weapons utilized (physical, of syntax and semantical).

This framework is easily operational in the various levels of organizational management, open to new technological innovations, easily supporting the re-engineering of the processes, integrating internal organizational methologies which can be easily read.

Key Terms: Information Warfare, Information Security Management, Analysis and Evaluation of Risk.

ÍNDICE

LISTA DE ABREVIATURAS

AM	___	Academia Militar
BS	___	Bristish Standard
C2	___	Comando e Controlo
C3I	___	Comando, Controlo, Comunicações e Informações
C4I	___	Comando, Controlo, Comunicações, Computadores e Informações
CDD	___	Centro de Dados da Defesa
CEM	___	Curso de Estado Maior
CIO	___	Chief information Officer
CIS	___	Communication and Information Systems
CISSP	___	Certified Information Systems Security Professional
CNA	___	Computer Network Attack
COBIT	___	Control Objectives for Information and Related Tecnology
DIMIL	___	Divisão de Informações Militares
DNS	___	Domain Name System
DoS	___	Denial of Service
ECDL	___	European Computer Driving Licence
FM	___	Fild Manual
GICI	___	Guerra de Informação / Competitive Intelligence
GNS	___	Gabinete Nacional de Segurança
HTTP	___	Hypertext Transfer Protocol
IAR	___	Identificação e Avaliação de Riscos
IDS	___	Intrusion Detection System
IEC	___	International Electrotechnical Commission
IEEE	___	Institute of Electrical and Electronics Engineers
IESM	___	Instituto de Ensino Superior Militar
IIS	___	Internet Information Server
IGeoE	___	Instituto Geográfico do Exército
INFOSEC	___	Information Security
INFO OPS	___	Operações de Informação
ISACA	___	Information Systems Audit and Controls Association
ISMS	___	Sistema de Gestão de Segurança da Informação
ISO	___	International Organization for Standardization
ITIL	___	Information Tecnology Infrastructure Library
JP	___	Joint Publication
LAN	___	Local Area Network
MAN	___	Metropolitan Area Network
MCSE	___	Microsoft Certified Systems Engineer
MDN	___	Ministério da Defesa Nacional
NAS	___	Network Attached Storage
NATO	___	North Atlantic Treaty Organization
NIST	___	National Institute of Standards and Technology
OCTAVE	___	Operationally Critical Threat, Assets, And Vulnerability Evaluation
OI	___	Operações de Informação
OSI	___	Open Systems Interconnection
PDCA	___	Plan-Do-Check-Act
PNPS	___	Políticas, Normas e Procedimentos de Segurança
SAN	___	Storage Area Network
SEGNAC	___	Segurança Nacional
SGSI	___	Sistema de Gestão de Segurança da Informação
SI	___	Sistemas de Informação
SIS	___	Serviço de Informações de Segurança
SLA	___	Service Level Agreement
SNTP	___	Simple Network Time Protocol
SWOT	___	Strenghts, Weaknesses, Opportunities and Threats.
TCP/IP	___	Transmission Control Protocol/Internet Protocol
TIC	___	Tecnologias da Informação e da Comunicação
UDP	___	User Datagram Protocol
UML	___	Unified Modelling Language
VPN	___	Virtual Private Network
WAN	___	Wide Area Network

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

GLOSSÁRIO

Os conceitos apresentados são a base teórica da dissertação, fornecendo a linguagem integradora dos assuntos abordados e para os quais apresentamos as principais definições:

AMEAÇA: a causa potencial de um incidente, do qual pode resultar prejuízo no sistema ou na organização (ISO/IEC 13335-1, 2004).

CONFIDENCIALIDADE: garantir que as informações sejam acessíveis apenas aqueles que estão autorizados a terem acesso (ISO/IEC 17799, 2005).

DADOS: factos discretos e objectivos relativos a acontecimentos, fáceis de estruturar, capturar e transferir.

DISPONIBILIDADE: garantir que os utilizadores autorizados tenham acesso às informações e activos associados quando necessário (ISO/IEC 17799, 2005).

GESTÃO DE RISCOS (dos Sistemas de Informação): processo de identificar, controlar e minimizar ou eliminar os riscos de segurança que podem afectar os sistemas de informação, a um custo aceitável (ISO/IEC 17799, 2005).

GUERRA DE INFORMAÇÃO: **c**onjunto de acções destinadas a preservar os nossos Sistemas de Informação da exploração, corrupção ou destruição, enquanto simultaneamente se explora, corrompe ou destrói os Sistemas de Informação a um Adversário/Inimigo. (Waltz, 1998).

INCIDENTE: é qualquer evento que não faz parte do funcionamento *standard* de um serviço e que provoca ou pode provocar uma interrupção no serviço ou uma redução na respectiva qualidade (MacFarlane e Rudd, 2003).

INFORMAÇÃO: é o significado construído a partir dos dados, ou seja, são dados em contexto, com relevância e propósito.

INTEGRIDADE: garantir que o conteúdo da informação e / ou os métodos de processamento não são modificados de forma inesperada (ISO/IEC 17799, 2005).

RISCO (em Segurança da Informação): é a possibilidade de uma ameaça explorar vulnerabilidades de um activo ou conjunto de activos, do qual pode resultar prejuízo no sistema. É medido em termos de combinação da probabilidade de um evento ocorrer (ex. uma ameaça explorar vulnerabilidades) e as perdas ou prejuízos causados num activo ou grupo de activos (ISO/IEC 13335-1, 2004).

VULNERABILIDADE: fraqueza de um activo ou conjunto de activos, que pode ser explorada por uma ou mais ameaças (ISO/IEC 13335-1, 2004).

INTRODUÇÃO

A Sociedade em Rede, baseada na plataforma das tecnologias da informação e comunicação, afecta essencialmente a economia, as empresas, o mundo das comunicações e as esferas do poder, surgindo uma sociedade em rede feita da formação de redes de poder, riqueza, gestão e comunicação (Castells, 2002).

Estas mudanças não surgiram de forma imediata, mas resultaram de vagas sucessivas que culminaram na actual sociedade de que a Internet é o suporte tecnológico, permitindo gerir toda a informação que circula na rede e respectivos nós, com base numa tecnologia flexível e redundante.

Até 1650 – 1750 podemos falar, tal como refere Toffler (1984), numa primeira vaga, em que a civilização agrária dominava o planeta e o principal meio de comunicação era especialmente o serviço mensageiro.

Após esta fase, surgiu a revolução industrial, uma segunda vaga que “abalou” todas as instituições e modificou o modo de vida de milhões de pessoas e em que os principais meios de comunicação eram: correio, telefone e *mass media* (comunicação de um para muitos).

Actualmente a transição para a terceira vaga requer a criação de um sistema de informação altamente ramificado e aberto. Este sistema de informação é a base tecnológica necessária para suporte da actual sociedade em rede.

Uma das principais consequências do aparecimento das redes de comunicação electrónica e da vasta utilização da Internet, foi a integração global dos mercados financeiros, o revolucionar do comércio electrónico entre as empresas, investidores e empresas, entre vendedores e compradores e, por fim, o próprio mercado das acções. Outra das consequências foi a remoção de níveis intermédios dos processos de compra e venda, reduzindo os custos para o comprador e o vendedor.

Uma das empresas pioneiras da organização empresarial em rede *on-line* foi a *Dell Computers*, que se tornou uma das líderes na indústria de computadores pessoais em virtude do seu modelo empresarial inovador, ou seja a *Dell* recebe os pedidos *on-line*, utilizando uma página *web* que permite aos clientes personalizar o seu produto, garantido simultaneamente a interactividade e flexibilidade na compra.

A Internet permitiu a globalização das empresas, favorecendo os intercâmbios e a produção de riqueza, mas simultaneamente introduziu novas vulnerabilidades, que podem ser exploradas por actores mal intencionados. Efectivamente, os sistemas de informação organizacionais, ligados com a «rede das redes», possibilitam uma troca de fluxos de informação que são susceptíveis de ser interceptados, manipulados ou destruídos (Boniface, 2002).

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).

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 infra-estrutura tecnológica ligada à Internet. Consequentemente face à Guerra de Informação / Competitive Intelligence, existe a necessidade de 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 da sua informação ou da que está sob a sua responsabilidade, deve a organização possuir uma política de segurança. É 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. É publicado e divulgado por todos os funcionários.

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.

Surge a necessidade da identificação e avaliação de riscos como processo dinâmico, que deverá ser conduzido periodicamente, de forma a manter actualizados os vários indicadores de uma possível *Framework* de Segurança[1] 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)".

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.

[1] 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.

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 SI e consequentemente a segurança da informação. É necessário dispor de indicadores realistas para minimizar as possíveis acções de Guerra de Informação / *Competitive Intelligence* sobre os SI.

Definimos Guerra de Informação como um "Conjunto de acções destinadas a preservar os nossos Sistemas de Informação da exploração, corrupção ou destruição, enquanto simultaneamente se explora, corrompe ou destrói os Sistemas de Informação a um Adversário / Inimigo […]" (Waltz, 1998, p.20). Já a *Competitive Intelligence* é um processo sistemático e ético de reunião, análise e gestão da informação, que pode afectar o planeamento, as decisões e as operações de uma organização (Taborda e Ferreira, 2002).

Uma *Framework* de Segurança da informação deve procurar integrar os principais *Standards* e suas metodologias de aplicação, as boas práticas da segurança da informação e de considerar uma rigorosa metodologia de identificação e avaliação de riscos, apresentando aos decisores das organizações uma visão macroscópica sobre a segurança da informação.

1. METODODOLOGIA DE INVESTIGAÇÃO

1.1 OBJECTIVOS

Pretendemos apresentar na dissertação uma *Framework* de Segurança para os SI das organizações militares (embora seja adaptável a outras), que caracterizamos de forma genérica na abordagem teórica apresentada. Estas actuam num ambiente de conflito e onde todo o risco tem que ser mitigado ao máximo. Procuramos reflectir nas suas dimensões, componentes e indicadores os possíveis controlos de segurança ou seja de defesa a implementar contra as possíveis operações de informação e que possam garantir as propriedades fundamentais da segurança da informação.

Adoptamos neste documento a definição de controlo do ISACA (Cobit, 2005), segundo o qual um controlo é uma política, procedimento, prática, ou estrutura organizacional desenhada de forma a proporcionar um razoável grau de certeza que os objectivos de negócio irão ser atingidos e que acontecimentos indesejáveis são prevenidos ou detectados e corrigidos.

A *Framework* de Segurança obtida deve permitir-nos integrar e orientar o esforço de uma equipa multidisciplinar, ligada a um "Departamento de Gestão da Segurança", cujas competências seriam de planear, coordenar a implementação, gerir e auditar a segurança dos SI nos seus múltiplos domínios, garantindo deste modo economia de esforços e acompanhamento com rigor do constante dinamismo e mutabilidade dos SI, reflexo da constante evolução tecnológica.

Em conclusão**,** esta deve permitir um nível de gestão e manutenção leve e ágil, integrando os controlos de segurança existentes na organização e permitindo responder com eficiência às constantes alterações nos processos existentes na organização militar, ou seja, na realidade a Framework de Segurança deve garantir a Gestão da Segurança da Informação reduzindo ao mínimo o risco de segurança nas dimensões de segurança propostas.

1.2 ORGANIZAÇÃO DA DISSERTAÇÃO

A tese encontra-se dividida em cinco capítulos, reflectindo a abordagem da metodologia de investigação aplicada.

Neste primeiro capítulo, apresenta-se a metodologia de investigação seguida, referindo as principais fontes de suporte científico da dissertação, integrando a visão académica baseada em modelos conceptuais, com uma visão mais pragmática e adequada à realidade das organizações. É formulada a questão central e as questões derivadas, sob a forma de uma pergunta de partida que apresente clareza, exequibilidade e pertinência de forma a orientar o trabalho de investigação e levantam-se as hipóteses.

No segundo capítulo, é demonstrada a importância do recurso informação e dos SI no contexto organizacional, definindo os conceitos de suporte ao tema da dissertação, com a integração na segurança da informação de uma perspectiva de Guerra da Informação / Competitive Intelligence. Os conceitos apresentados, são independentes de qualquer tipo de organização, da sua dimensão, da sua natureza pública ou privada e dos recursos de TI.

No terceiro capítulo, são identificadas as dimensões, componentes e indicadores da *Framework* de Segurança mais relevantes na nossa opinião e propõe-se uma metodologia de análise de ameaças.

No capítulo quatro, é apresentada a *Framework* de Segurança final, descrevendo o seu modelo de Gestão da Segurança da Informação e introduzindo os instrumentos metodológicos de validação utilizados na dissertação: um inquérito e uma auditoria a um SI de uma organização militar. Como corolário, são apresentadas as conclusões e possibilidades futuras de estudos no capítulo cinco.

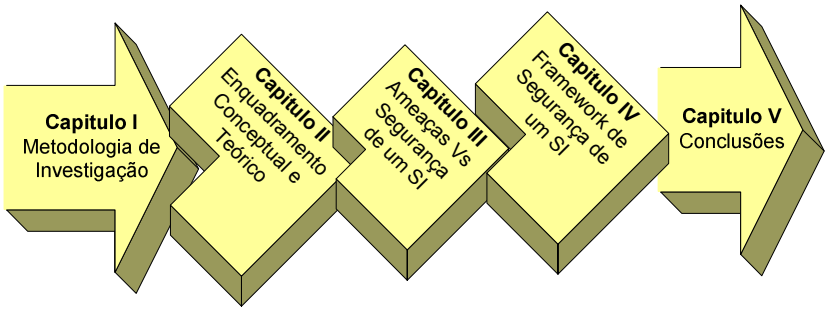
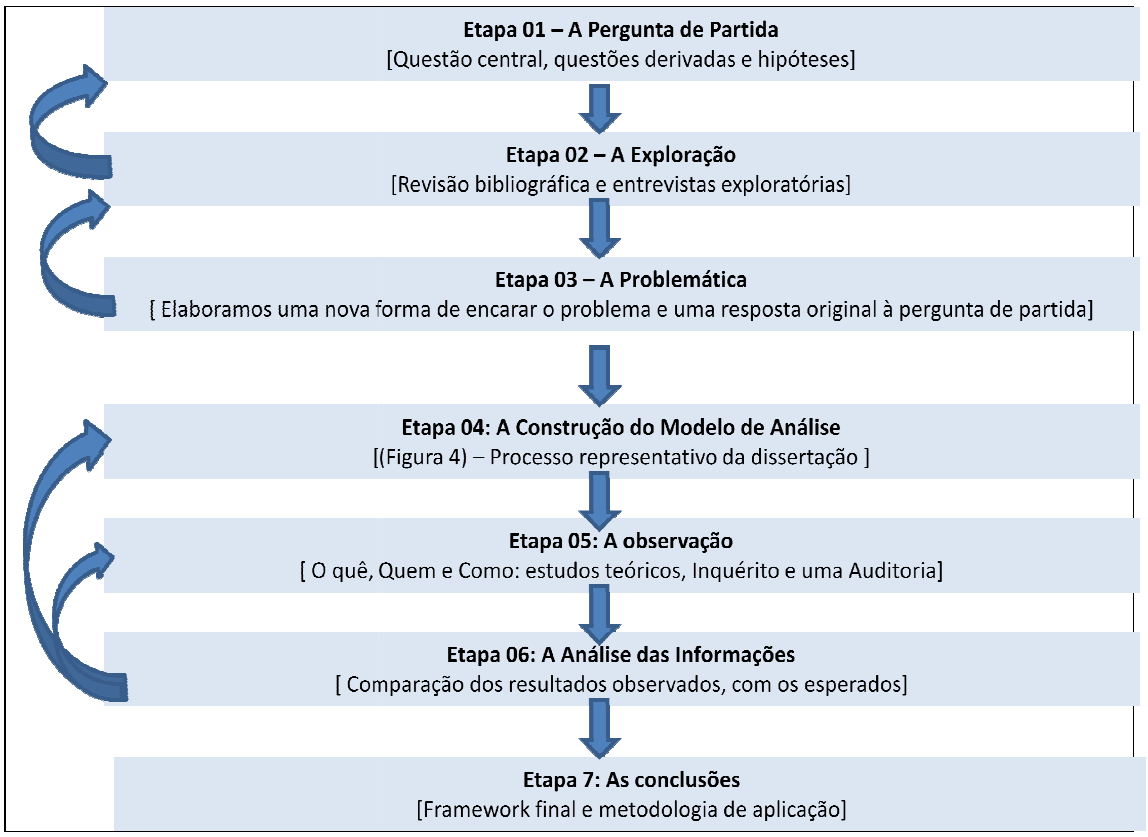


Figura 1 – Organização da Dissertação

1.3 FORMULAÇÃO DO PROBLEMA

A metodologia de investigação seguida na dissertação, obedece ao esquema apresentado na Figura 2, não sendo apenas apresentado como uma simples soma de técnicas, mas como um método de trabalho em sentido lato, tendo sido necessário a adaptação ao problema da dissertação. Assim, após a formulação da pergunta de partida, foi efectuada uma revisão bibliográfica, tendo em vista conhecer as várias tentativas de resolução feitas até à presente data. Posteriormente elaborou-se uma nova forma de encarar o problema e foi proposta uma resposta original à pergunta de partida. Por fim foram validadas as hipóteses através da aplicação da metodologia a um caso de estudo e foram extraídas as conclusões.



Fonte: Adaptado de Quivy e Campenhoudt (2005, p. 27)

Figura 2 – Metodologia de Investigação

A questão central à qual pretendemos responder é a seguinte – Será possível construir uma Framework de Segurança para uma organização do tipo Militar que permita garantir a segurança dos Sistemas de Informação e da sua Informação, face às acções de Guerra de Informação / Competitive Intelligence?

Apesar de na essência a dissertação apresentada ser um estudo teórico, procuramos validar a *Framework* apresentada com a sua aplicação a um caso particular do Centro de Dados da Defesa, face à necessidade de avaliação de segurança do SI deste *datacenter* (âmbito), fornecendo consequentemente uma possível metodologia de Gestão da Segurança da Informação aos seus decisores.

Para responder à questão central levantamos duas questões derivadas:

Na primeira – quais as dimensões e componentes mais relevantes para garantir a segurança de um SI e da Informação? - procuramos enunciar os principais critérios para construir o conceito de segurança do SI.

Através da segunda questão – quais os indicadores mais relevantes que devem ser utilizados em cada um dos componentes? - procuramos obter os atributos ou características de cada dimensão, facilmente observáveis e que permitem operacionalizar a implementação do conceito de segurança do SI.

Nesta abordagem levantamos como hipótese a existência de quatro dimensões de segurança. Ou seja, para garantir a segurança da informação necessitamos de analisar o problema em cada uma das dimensões Organizacional, Física, Pessoal e Tecnológica, que representamos através da Figura 3.

Figura 3 – Hipóteses para as Dimensões

As dimensões indicadas (Organizacional, Física, Pessoal e Tecnológica), resultam da percepção dos decisores para a probabilidade de Ataques às Redes de Computadores (Dimensão Tecnológica), particularmente vulneráveis a ataques de negação de serviço (DoS), pela possibilidade de Destruição Física (Dimensão Física), que como o próprio nome indica, consiste na destruição física, por meios físicos ou electrónicos do alvo e pela Gestão das Percepções (Dimensão Pessoal) ou seja acções que visam influenciar audiências específicas, nas quais são usadas combinações das outras capacidades de forma coordenada (operações psicológicas, propaganda, decepção), que visam minar a vontade do adversário.

A segurança das dimensões Organizacional, Física, Pessoal e Tecnológica, pretende barrar os principais métodos de ataque à organização. É fundamental a correcta análise da estrutura e dinâmica dos SI organizacionais, de modo a garantir o eficiente planeamento e implementação da Framework de Segurança.

1.4 REVISÃO BIBLIOGRÁFICA

Apresentamos nesta secção as principais fontes de suporte teórico e prático[2] da dissertação. Procuramos consultar especialistas e empresas relacionadas com esta temática, consolidando a *Framework* de Segurança apresentada, integrando uma visão académica, com uma visão mais pragmática adequada à realidade das organizações, dos gestores e dos responsáveis pelos SI.

Em termos de Metodologia de Investigação, seguimos o modelo para as Ciências Sociais apresentado por Quivy e Campenhoudt (2005) e procuramos reflectir as "boas práticas" na elaboração e aplicação de Inquéritos com base nos conceitos apresentados por Ghiglione e Matalon (2001).

No enquadramento conceptual dos Sistemas de Informação, analisamos uma das referências para a gestão de SI, Laudon e Laudon (2006) e na Gestão de TI recorremos na essência à análise dos dez processos base da ITIL, como *Framework* adaptável das melhores práticas que promovem a qualidade nos serviços de IT.

Para a análise de Processos, recorremos à Norma Portuguesa EN ISO 9001 (2000) – Sistemas de gestão da qualidade, requisitos. Nas Técnicas de Análise do Negócio recorremos a Cunha (2001) e para os Modelos de Gestão e Competitividade a Sarmento (2005).

A área da Guerra de Informação e Operações de Informação, foi suportada pelos modelos conceptuais apresentados por Waltz (1998), na doutrina NATO e dos Estados Unidos da América. Na Competitive Intelligence consideramos as orientações e os conceitos referidos por Taborda e Ferreira (2002).

Em termos de Segurança da Informação[3], analisamos as normas e instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática (SEGNAC's). Efectuamos a análise da ISO / IEC 17799 (2005), como

[2] Em termos de Entidades / Empresas consultamos o Gestor da Unidade de Negócio da Segurança da Informação da SINFIC (Sr. Fernando Fevereiro Mendes) e o responsável pela Divisão de Administração e Comunicação e Segurança do Centro de Dados da Defesa (Tenente Coronel Eng.º António Galindro). Recorremos à experiência pessoal obtida como membro do grupo de delegados / auditor interno do Instituto Geográfico do Exército para a Certificação na ISO 9001:2000 e 14001:1999 e administrador de redes informáticas e programador durante os últimos cinco anos.

[3] Consolidado com o curso "Segurança de Matérias Classificadas" no Gabinete Nacional de Segurança e o *Implementing ISO 27001: 2005 Course da BSI Management Systems* na Empresa SINFIC.

referencial às boas práticas de segurança da informação em dez áreas chave (com origem na BS 7799 – 1 publicada em 2000 e com revisão em 2005 e em 2007 a ISO / IEC 17799: 2005 passou a ISO / IEC 27002).

Para a Análise e Avaliação do Risco, tomamos em consideração:

- A BS 7799 – 3 (2006), terceira parte da BS 7799, que define as linhas orientadoras para a gestão de risco da segurança da informação.
- A ISO / IEC TR 13335-3 (1998), este *standard* publicado em 1998 incide sobre a análise de risco e apresenta um método que em parte foi subscrito por vários especialistas na implementação de um Sistema de Gestão da Segurança da Informação.
- A metodologia de gestão de risco do organismo de *standards* dos EUA **(**NIST SP 800-30, 2001**)**.

Na Segurança Informática**,** a dissertação teve como base:

- As orientações teóricas referidas por kurose e Ross (2008).
- Os conceitos essenciais para obtenção da certificação *CISSP* indicados por Tittel et al (2003).

Em termos do "Estado da Arte" após a revisão bibliográfica efectuada, podemos considerar que a segurança da informação deve ser uma prioridade para os gestores das organizações (incluindo os das empresas públicas), sendo desejável uma *Framework* que os ajude no esforço de gestão da segurança da informação.

No âmbito da Segurança dos Sistemas de Informação, diversos *standards*, códigos de boas práticas, certificações e metodologias de implementação associadas poderão ser utilizadas considerando as suas especificidades (Solms e Eloff, 2000) e das quais se referem as seguintes, após a revisão bibliográfica efectuada:

- As directivas de segurança da NATO**,** para implementar nas suas organizações militares, de acordo com documentos classificados.
- A norma ISO / IEC 27001 (2005), que apresenta os requisitos necessários para implementar um Sistema de Gestão da Segurança da Informação e que procura apresentar uma base de conhecimento comum sobre a segurança de Sistemas de Informação (Santos, 2006).

- As recomendações do *Nacional Institute of Standards and Tecnology*, através do guia para a segurança de sistemas de informação suportados em tecnologia (NIST SP 800-26, 2001) e das orientações para efectuar testes em redes informáticas de modo a identificar as suas vulnerabilidades (NIST SP 800-42, 2001).
- A metodologia OCTAVE, que consiste num 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).
- A ISO / IEC TR 13335-4 (1998) na qual são apresentados alguns dos principais controlos tecnológicos a considerar para fazer face aos mais relevantes ataques sobre os SI e a ISO / IEC TR 13335-5 (2001) que se foca nos controlos tecnológicos a aplicar para a segurança das redes e comunicações.
- A ISO / IEC 15408 (2005), consiste em três partes e que conforme refere Santos (2006) é destinada essencialmente a definir um conjunto de critérios que permitem avaliar um sistema de segurança. Esta norma é uma adaptação directa da segunda versão da norma CC (Common Criteria), que actualmente se encontra na versão três e também ela constituída por três partes.
- O COBIT (2005), como metodologia de controlo interno de divulgação internacional, especificamente vocacionado para aspectos de controlo relacionados com SI (Solms e Eloff, 2000; Ferreira, 2001).

Em conclusão, dos vários *Standards* (de nível Internacional, Nacional ou Organizacional), códigos de boas práticas, listas de controlos, certificações existentes para a segurança da informação podemos encontrar desde abordagens mais focadas nas tecnologias ou em processos de negócio. Podendo estas ou outras designações ser enquadradas numa *Framework* hierárquica para a segurança da informação (Solms e Eloff, 2004). No entanto face à especificidade da organização militar e dos SI que suportam o C2, procuraremos uma *Framework* operacional e flexível.

1.5 PROBLEMÁTICA E MODELO DE ANÁLISE

O modelo de análise apresentado (Figura 4), segue uma metodologia para aplicação que se centra na organização como um todo, em virtude da Framework de Segurança da Informação proposta, se basear na análise dos fluxos de informação que suportam os processos organizacionais. Na realidade, mais que uma metodologia de identificação e avaliação do Risco[4], é uma Framework de defesa contra os possíveis métodos de ataque a realizar aos SI e uma possível Metodologia de Gestão da Segurança da Informação para organizações do tipo Militar.

A abordagem na construção da Framework centra-se mais na perspectiva do ataque e defesa sobre os SI e menos na avaliação do Risco, embora sujeita a ligeiras modificações possa contribuir para o mesmo efeito. Na nossa metodologia de aplicação a probabilidade de uma ameaça explorar uma vulnerabilidade é igual para todos os cenários e o seu impacto (custos financeiros vs imagem vs legais) resulta dos cálculos efectuados pela organização *à posteriori*.

Apoiamo-nos em três fases principais para a sua construção, as quais passamos a descrever:

Na primeira fase procuramos obter uma tipologia de ameaças e as dimensões, componentes e indicadores associados ao conceito de segurança de SI, tendo por base a consulta documental a fontes científicas ou seja a recolha de dados preexistente.

A segunda fase permite-nos validar algumas das dimensões, componentes e indicadores de segurança mais relevantes, fundamentalmente através de um estudo exploratório referente à percepção para a conflitualidade da informação em elementos da organização militar, a uma auditoria ao Centro de Dados da Defesa e pela análise do Plano de Emergência Interna do IGeoE.

Na terceira fase apresentaremos a *Framework* de Segurança utilizando o diagrama de classes da *UML*, que permitirá apoiar na escolha e prioritização de controlos para garantir a segurança da informação organizacional.

[4] Podemos analisar com profundidade algumas das mais importantes metodologias de Gestão de Riscos de SI em Ferreira (2001).

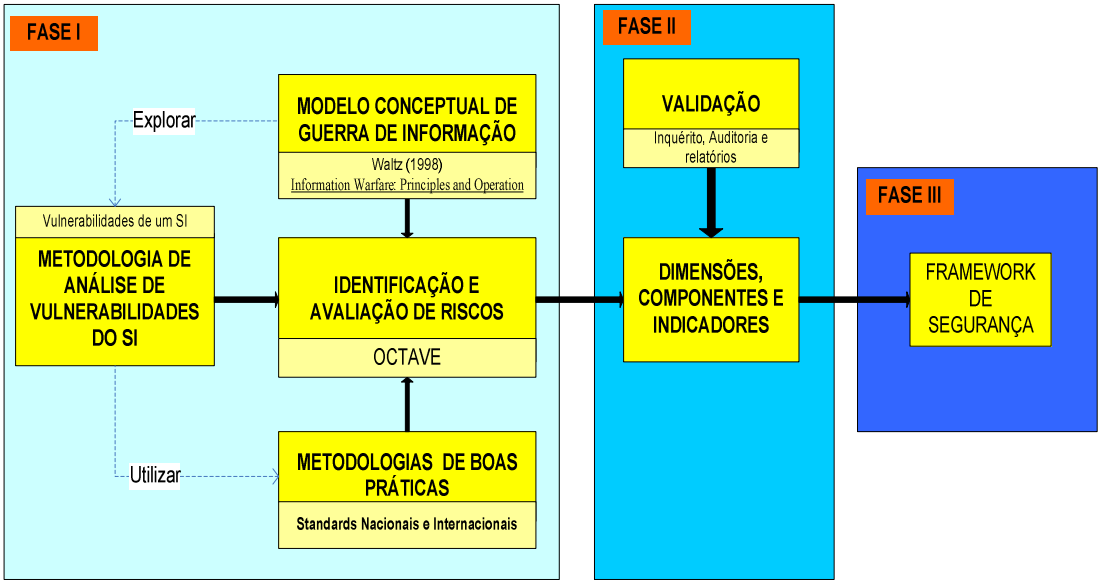


Figura 4 – Modelo de Análise

Na análise interna da organização, é fundamental suportar com rigor a descrição de cada um dos anéis da metodologia de análise de vulnerabilidades dos SI organizacionais apresentada na Figura 5, com base nas "melhores práticas actuais".

Como podemos observar (Figura 5), devemos considerar a análise dos processos de negócio, suportados em processos de TIC, em que ambos possuem vulnerabilidades, em comparação com as melhores práticas apresentadas (ex. ITIL). Após o que devemos efectivar a gestão da segurança da informação, como refere a ISO 27001 (2005).

No entanto a implementação de um novo processo, deverá na sua fase inicial de análise e desenho considerar a gestão da segurança da informação, garantindo que após a sua operacionalização, este processo garanta as três propriedades fundamentais da segurança.

Neste modelo de análise, a metodologia OCTAVE baseada em processos, permite-nos a identificação e avaliação de riscos, orientando o esforço de sistematização e garantindo que os principais passos serão efectuados na nossa metodologia de obtenção de vulnerabilidades e suporte da *Framework* de Segurança.

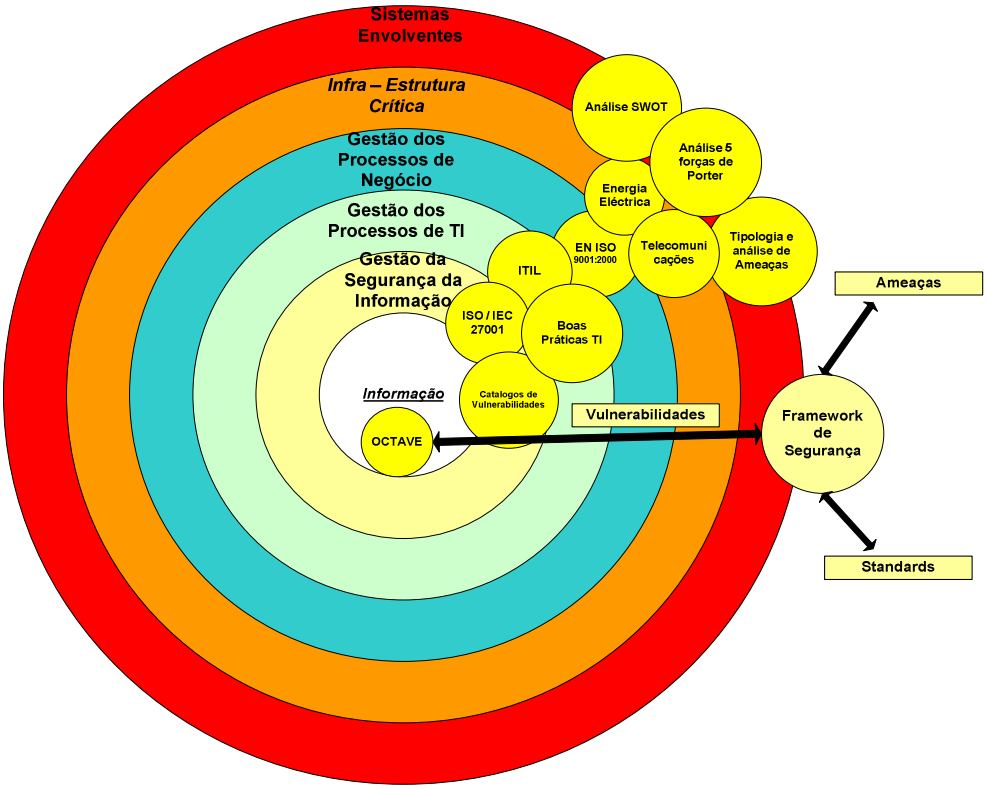


Figura 5 – Metodologia de Análise de Vulnerabilidades de um SI

Após a sistematização indicada nas Figuras 4 e 5, o modelo conceptual de validação apresentado na Figura 6, efectua a abordagem teórica para resolver o problema formulado pela pergunta de partida.

Provando as hipóteses indicadas, respondemos deste modo às questões derivadas e à questão central e consequentemente garantimos a construção de uma Framework de Segurança.

Para validar cada uma das hipóteses tomamos em consideração para além de referências académicas, os padrões internacionais produzidos pela ISO, as orientações de nível Nacional referidas nos SEGNAC´s, procurando introduzir face à especificidade das organizações militares a visão para a segurança dos SI do Exército Português e da NATO.

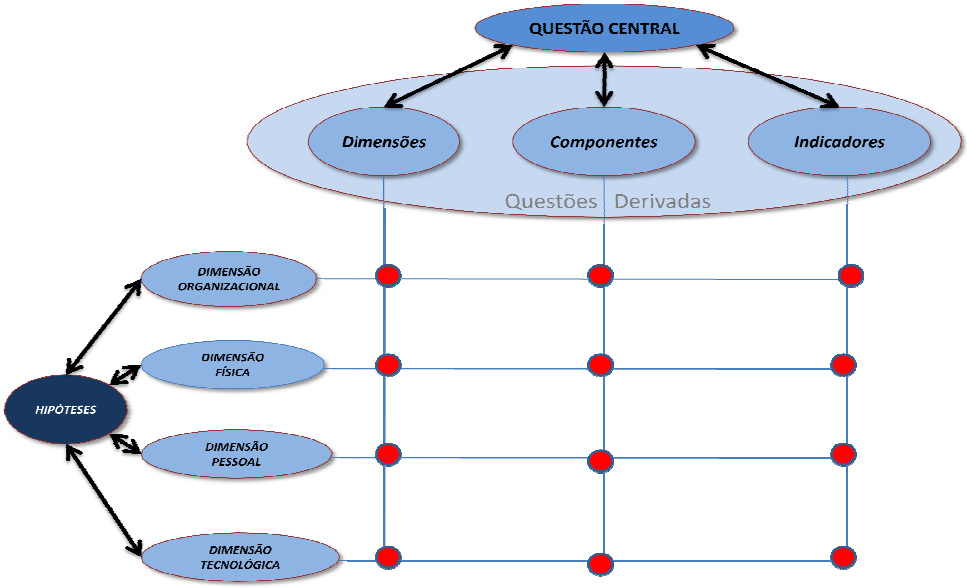


Figura 6 – Modelo Conceptual de Validação da Problemática

Em conclusão, procuramos com a dissertação acrescentar em termos originalidade para as actuais *Frameworks* de Segurança de SI e suas metodologias de aplicação, os seguintes aspectos:

- Desenvolver e apresentar uma tipologia de identificação e análise de ameaças integrando a perspectiva militar, de modo a fazer face a uma possível Guerra de Informação levada a efeito por actores mal intencionados, que possam afectar as infra-estruturas e recursos de informação do Estado.

- Apresentar uma *Framework* de Segurança operacional e flexível, que permita integrar algumas das metodologias já existentes nas organizações, com implicações na segurança dos SI, permitindo deste modo atingir objectivos de segurança mais rapidamente e com maior eficiência.

- Utilizar a linguagem de modulação *UML* (Diagrama de Classes) para representar o modelo conceptual de Segurança, de modo a transmitir ao decisor os serviços ou a especificação da Segurança dos SI e não os detalhes da sua implementação. Procura-se assim integrar alguns dos conceitos já validados e aceites pelos gestores, garantido desta forma que a sua percepção os leve a tomar as decisões correctas de acordo com a garantia da segurança global dos SI.

2. ENQUADRAMENTO CONCEPTUAL E TEÓRICO

Apresentamos neste capítulo os conceitos de suporte à dissertação, perspectivamos as possíveis acções de Guerra de Informação / Competitive Intelligence sobre os Sistemas de Informação organizacionais, independentemente do tipo de organização, da sua dimensão, natureza pública ou privada e dos recursos em tecnologias da informação e comunicação, simultaneamente constatamos a importância do recurso informação e da sua segurança. As próximas secções são essenciais para a compreensão das dimensões, componentes e indicadores identificados e apresentados na *Framework* de Segurança proposta nesta dissertação.

AS ORGANIZAÇÕES E OS SISTEMAS ENVOLVENTES

As organizações enquanto "entidades complexas" integradas numa sociedade em rede, funcionam na sua maioria com base em processos formais ou *ad-hoc*, apoiados em fluxos de informação, manuseados por pessoas e suportados numa infra-estrutura tecnológica ligada à Internet.

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), "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, permitem 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 agir no ambiente de informação das organizações.

Após a análise externa, 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 DOS SI 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 reúnam ou procuram, processam, armazenam e distribuam 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 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 (Figura 7). A relevância desse critério é apontada por Amaral (1994) ao afirmar que "A importância da diferenciação dos diversos tipos de SI resulta do facto deles desempenharem papéis diferenciados quando são envolvidos como objecto de atenção nas actividades de planeamento, desenvolvimento, exploração e gestão do SI global da organização".

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

Figura 7 – Níveis de uma Organização

Apesar de este ser unanimemente aceite como modelo conceptual representativo dos níveis de gestão de uma organização, no propósito deste trabalho parece-nos ser mais eficiente, para a identificação e análise de vulnerabilidades e controlos de segurança, o modelo que apresentamos na Figura 8, face à transversalidade dos processos e das tecnologias da informação e comunicação que suportam as actividades da organização, nos seus diversos níveis.

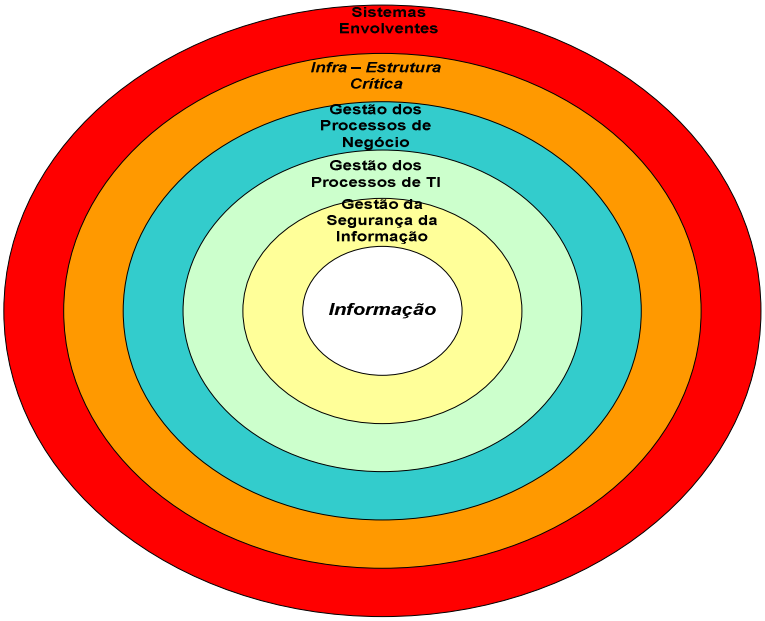


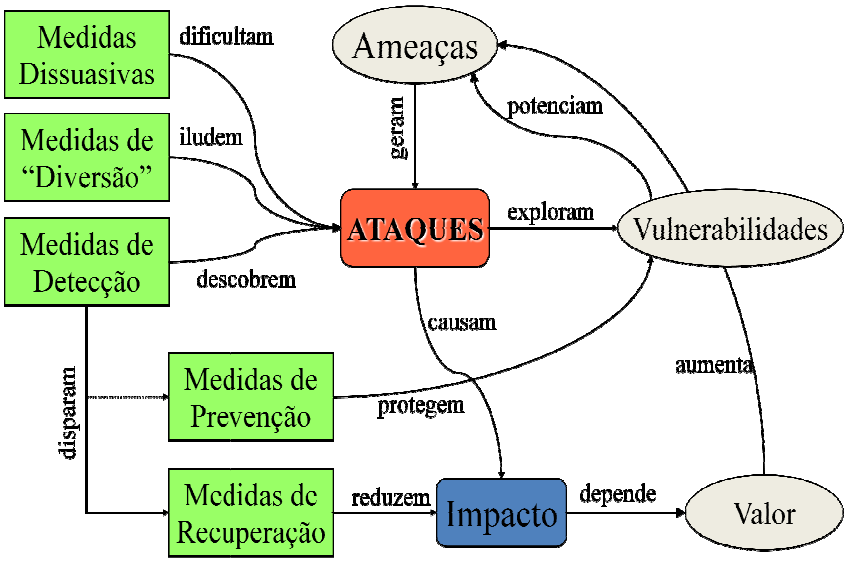
Figura 8 – Modelo de Análise de uma Organização

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 9, de simplificação conceptual e facilidade de integração com outras metodologias, onde a questão chave parece-nos ser a sua operacionalização.



Fonte: Adaptado de Santos (2006)

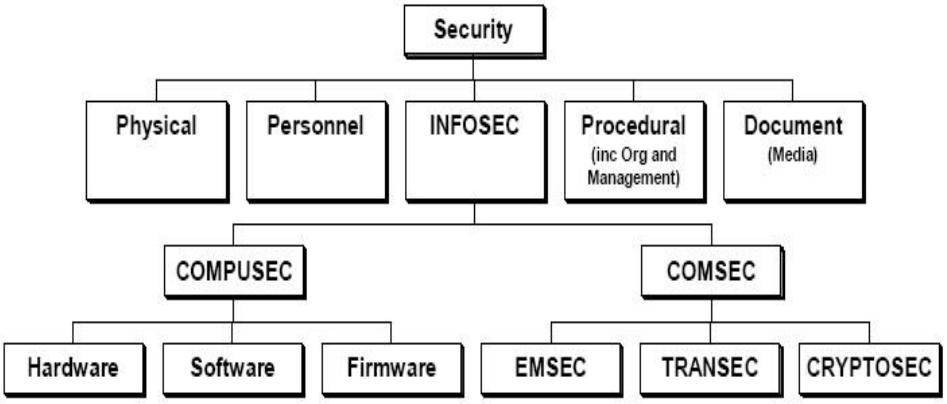
Figura 9 – Modelo de suporte à norma ISO / IEC 17799

A aplicação deste modelo de segurança da informação, exige fundamentalmente a correcta identificação das ameaças, vulnerabilidades e a cenarização 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 semelhante, com uma abordagem mais militar e que podemos observar na Figura 10, 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. Neste modelo não se consideram as questões relacionadas com a gestão do risco.

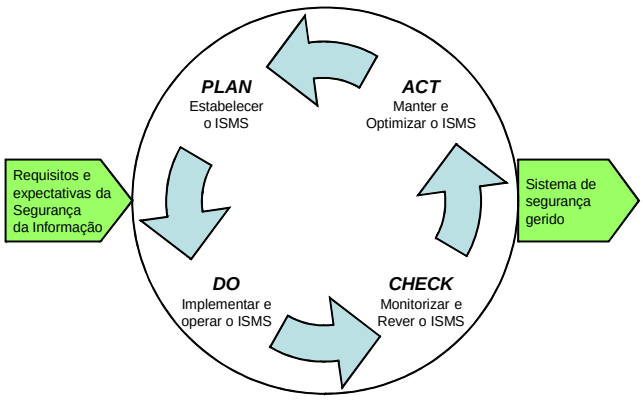


Fonte: INFOSEC (2004, p. v-1-4)

Figura 10 – Modelo de Segurança da NATO

No entanto, qualquer dos modelos sugeridos ou futuramente desenvolvidos deve ainda enquadrar-se com a utilização de um modelo de processo conhecido como PDCA (ISO / IEC 27001, 2005), à semelhança do que é adoptado nas normas ISO 9001 e ISO 14001, o qual se encontra ilustrado na Figura 11.

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).



Fonte: Adaptado da ISO / IEC 27001 (2005)

Figura 11 – Modelo PDCA para um ISMS

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 [5] para identificar e avaliar o risco de segurança, utilizadas em organizações militares e civis, das quais salientamos:

- Ao nível dos *standards* Internacionais a ISO/IEC TR 13335-3 (1998); ao nível dos *standards* Nacionais a BS 7799-3 (2006) e a do organismo de *standards* dos EUA (NIST 800-30, 2001).

- A nível académico a metodologia OCTAVE. Desenvolvida no *Software Engineering Institute da Carnegie Mellon University*, preconiza um processo de sessões onde os colaboradores que trabalham na área analisada da organização definam 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.

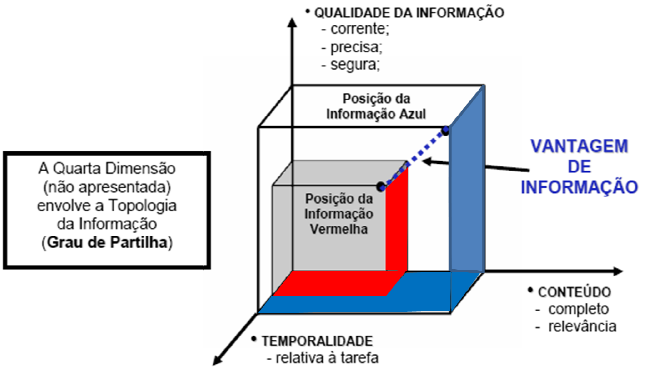
[5] Descritos alguns modelos utilizados nas organizações militares por Rosa (2003) e alguns aplicados nas organizações civis em Ferreira (2001).

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 Nunes (2005) e Alberts et al (1999), que são as que seguiremos neste trabalho.

Nesta abordagem, o valor da informação é determinado segundo as dimensões (Qualidade, Temporalidade e Conteúdo), como mostra a figura 12. 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 da informação "azul"), garantindo a permanente segurança da informação.

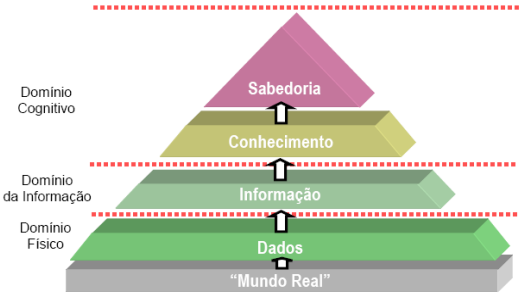
O objectivo a atingir pela organização "azul" será o de aumentar tanto quanto possível o diferencial existente no domínio da informação relativamente à organização "vermelha", convertendo depois essa assimetria numa vantagem operacional (Nunes, 2005).



Fonte: Adaptado de Alberts et al (1999, p. 34).

Figura 12 – Superioridade de Informação

Uma outra abordagem possível é a inspirada nos sistemas de Comando e Controlo (C2), que consideram os domínios ilustrados na figura 13. Estes domínios são utilizados porque 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 NATO SAS-050 (2006, p.91).

Figura 13 – 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.

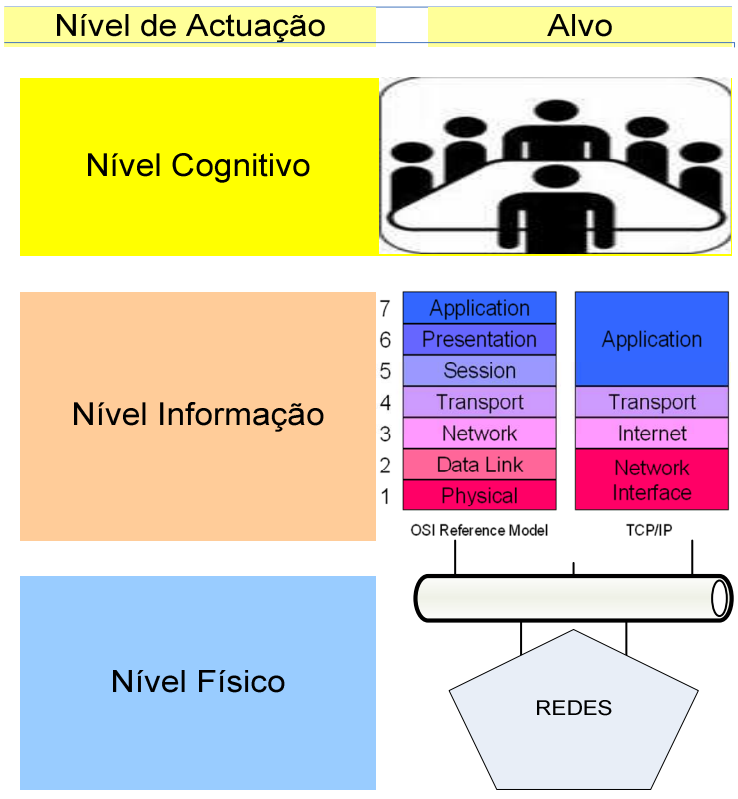
A visão militar de C2 tem por suporte os conceitos de Comando como a autoridade investida num indivíduo, para dirigir, coordenar e controlar uma força militar e o Controlo definido como a autoridade exercida por um Comandante sobre parte das actividades das organizações subordinadas, ou outras organizações 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.

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 (Figura 14) que seguiremos neste trabalho, as possíveis acções que podem ser aplicadas aos vários níveis do sistema de informação. Neste modelo, esse sistema consiste no "conjunto de indivíduos, organizações e sistemas que procedem à recolha, processamento, disseminação e actuação sobre a informação" (JP 3-13, 2006, p. I-1).

Na análise do ambiente de informação (designação usada neste contexto), 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).



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

Figura 14 – Modelo Operacional das OI

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 INFO OPS, foi criado o grupo de trabalho RTG SAS-057 [6] que analisou documentação de diferentes Países / Organizações (Bélgica, Canada, Alemanha, Holanda, Noruega, Suécia, Reino Unido, Estados Unidos da América, OTAN, União Europeia, MNIOE [7]), tendo elaborado o seu relatório final em Outubro de 2006.

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 USA e NATO utilizados nas Operações de Informação que servem de referência à dissertação 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.

[6] *Research and Technology Group*, do *System Analysis and Studies* (SAS – 057), que analisou doutrinas, políticas, conceitos, W*hitepapers*, publicados desde 1996.

[7] *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.

- Existe uma lista de capacidades disponíveis[8] e actividades relacionadas, que podem ser aplicadas para a obtenção directa ou indirecta dos efeitos pretendidos com as INFO OPS [9] e que são:

  - 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;

  - Actividades Anti-Comando, dirigidas à infra-estrutura de C4I de potenciais entidades adversárias;

  - Actividades de Informação, com vista a obter informações necessárias ao planeamento e execução de INFO OPS e a proteger os decisores e as capacidades das nossas forças; e

  - Actividades 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 e a guerra electrónica, complementadas pelas actividades de protecção das comunicações e dos Sistemas de Informação, com a finalidade de negar informação ao inimigo. 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).

Considerando que actualmente a maioria dos métodos de ataques são executados usando as redes informáticas (Hildreth, 2001; Richardson, 2007; Martins e Nunes, 2008), é essencial a análise e compreensão do seu funcionamento.

[8] Tendo em consideração as funções das INFO OPS 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.

[9] A categorização das actividades de INFO OPS apresentada segue a doutrina do Reino Unido, expressa no Joint Warfare Publication 3.80 de Junho de 2002, por ser considerada pelo RTO-TR_SAS 057 a de melhor compreensão.

CONCEITOS FUNDAMENTAIS DE REDES

Na dissertação vamos usar o termo "rede de computadores", quando quisermos falar 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 LAN, o cabo e os *hosts* 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 taxionomia 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 chamados *routers*, chamamos ligação inter-redes[10] 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 uma conjunta 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 utilizamos é o modelo TCP – IP, utilizado na Internet.

[10] Um exemplo comum é um conjunto de LAN´s conectadas por uma WAN.

Nas redes é essencial garantir a segurança do perímetro, como limite fortificado da nossa rede, que pode incluir normalmente os seguintes dispositivos: *routers*, *Firewalls*, *IDS* e dispositivos de VPN (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, configurações correctas e simultaneamente garantir-se as cópias de segurança da informação dos clientes.

CONCLUSÃO

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 para 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, têm por premissa o garantir o nível mais elevado de segurança, em todas as dimensões da segurança da informação.

Para construir uma Framework de segurança 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).

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

As análises apresentadas nesta secção 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), permitindo fornecer simultaneamente aos decisores um Modelo de Gestão da Segurança da Informação.

3. AMEAÇAS Vs SEGURANÇA DE UM SI

Neste capítulo pretendemos obter uma possível tipologia de ameaças e identificar e enunciar as dimensões, componentes e indicadores principais associados ao conceito de segurança do SI, definindo simultaneamente os conceitos de ameaça e vulnerabilidade.

3.1 TIPOLOGIA DAS AMEAÇAS

A sociedade em rede evolui a um ritmo acelerado e apresenta novas ameaças aos Sistemas de Informação das organizações. A Internet como suporte tecnológico da sociedade em rede, provoca alterações de poder, em virtude de suportar o ciberterrorismo, a cibercriminalidade e fundamentalmente a *cyberwarfare* (Hildreth, 2001).

Esta é o elemento estruturante da Sociedade em Rede e as ameaças aos sistemas de informação empresariais e militares surgem de governos estrangeiros, *hackers* e organizações criminosas via Internet. Na realidade a Internet "*derrubou fronteiras*"constituindo hoje o melhor suporte para desenvolver acções de Guerra de Informação (Nunes, 1999).

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.

Aproveitando o ciberespaço, a cibercriminalidade assenta no acesso indevido a sistemas computorizados para obter informações e no uso do computador e das redes virtuais para a obtenção do lucro ilegal. No entanto, a pornografia infantil e a sua exploração comercial através da *Web*, é actualmente um dos crimes que mais preocupa a justiça em todo o mundo, devido à dimensão que o negócio atingiu e aos elevados lucros que gera (Morgado e Vegar, 2006).

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).

PRIMEIRA ITERAÇÃO DE ANÁLISE DE AMEAÇAS

Na primeira iteração e devido à necessidade da tipificação das ameaças ser independente do tipo de organização (Civil & Militar), sua dimensão, natureza pública ou privada e dos recursos de tecnologias da informação, optamos por apresentar uma visão estratégica que permitisse facilmente enquadrar o desenvolvimento de um ataque estratégico com todos os seus possíveis desenvolvimentos ao nível operacional e táctico.

Consideramos no entanto que uma ameaça de nível táctico pode através de um método de ataque explorar vulnerabilidades de uma infra-estrutura e causar um impacto de nível estratégico.

As ameaças[11] que operam no ambiente de informação, de acordo com a orientação doutrinária dos EUA (*FM 3 – 13*, 2003, p.1-4) são classificadas de acordo com as suas capacidades da seguinte forma:

[11] Existem outras classificações como seja a apresentada pela NATO, que divide as ameaças aos CSI, em três tipos: internas, externas e acidentes naturais (INFOSEC, 2004, p. v-1-3).

- Primeiro Nível – Amadores, sozinhos ou em pequenos grupos, usando ferramentas e técnicas de *hacking* comuns, de um modo não sofisticado e sem apoio significativo.
- Segundo Nível – Indivíduos ou pequenos grupos com o apoio de entidades empresariais, sindicatos do crime, ou outros grupos transnacionais, usando ferramentas de *hacking* comuns de forma já algo sofisticada. Este nível de adversários inclui terroristas e organizações terroristas não governamentais. As suas actividades incluem espionagem, recolha de informação, levantamento e reconhecimento de redes e roubo de informação.
- Terceiro Nível – Indivíduos ou pequenos grupos apoiados por instituições estatais (civis ou militares) e por recursos significativos, usando ferramentas sofisticadas. As suas actividades são idênticas às do segundo nível.
- Quarto Nível – Operações de Informação conduzidas por Estados, especialmente através de *Computer Network Attacks* (CNA), usando as ferramentas mais avançadas e técnicas de decepção conduzidas em coordenação com operações militares.

SEGUNDA ITERAÇÃO DE ANÁLISE DE AMEAÇAS

Numa segunda iteração para a análise de ameaças, focamos na gestão organizacional, para a qual existem dezenas de modelos, que permitem reduzir a complexidade e as incertezas para a resolução dos problemas organizacionais (Steven et al, 2003). Dois dos modelos que gestores de todo o mundo consideram dos mais úteis no seu trabalho diário e que poderão ser utilizados para efectuar uma análise estratégica da organização na perspectiva da identificação e análise de ameaças são: o método de análise *SWOT* e o das cinco forças de *PORTER.*

No método de análise *SWOT*, uma organização efectua um planeamento estratégico, onde avaliará as suas forças e fraquezas, combinando com um levantamento das suas oportunidades e ameaças, sendo este ideal para uma auto-avaliação da administração (Steven et al, 2003). Este método permite ser facilmente integrado na nossa *Framework* de Segurança, permitindo com simplicidade e eficiência transmitir aos decisores, quais os seus pontos fortes e fracos em termos de segurança da informação dos SI organizacionais e simultaneamente apresentar as ameaças à sua missão.

O modelo de análise competitiva das cinco forças de Porter, permite enfatizar as forças competitivas externas em relação à nossa organização. Tendo consequentemente como indicadores a vigiar: os competidores existentes, novos participantes, compradores, fornecedores e possíveis substitutos, na perspectiva da conflitualidade da informação (a competição é garantida).

A combinação destes dois modelos, pode resultar numa identificação e análise de ameaças interna e externa realista e rigorosa face à perspectiva da utilização conflitual da informação, levando à percepção de todo o espectro de ameaças à organização, mais focado em pessoas e organizações.

TERCEIRA ITERAÇÃO DE ANÁLISE DE AMEAÇAS

A terceira iteração, permite-nos classificar algumas ameaças intrínsecas aos próprios componentes dos SI, utilizando a taxionomia apresentada por Pfleerger e Pfleerger (2007) e que consta no seguinte:

- Pela interrupção do serviço, atingindo a Disponibilidade através da:
  - Destruição, danificação, ou contaminação.
  - Recusa ou atraso, no acesso.
  - Deslocamento ou obscuração.
- Pela modificação, atingindo a Integridade por meio de:
  - Inserção ou produção de dados falsos.
  - Substituição, remoção, separação ou reordenação.
  - Representação ou codificação.
  - Repúdio.
- Pela intercepção, atingindo a Confidencialidade por meio de:
  - Cópia ilícita, observação, monitorização, ou inferição.
  - Transferência de controlo ou custódia.
  - Divulgação (em particular através de utilizadores legítimos, por negligência ou por fraude).

Na dissertação também englobamos nas ameaças as catástrofes naturais, pois pressupõem um conjunto de riscos naturais sobre um determinado componente ou componentes dos SI organizacionais, que podem ter impacto nos seus processos de negócio e na sua estrutura física (Solms e Posthumus, 2005).

Para determinar a possibilidade de actuação das ameaças de nível estratégico, utilizamos a metodologia da análise de actores, validada num exercício de simulação de gestão de crises – *Day After* – [12], permitindo determinar o perfil de cada actor (Anexo A).

MÉTODOS DE ATAQUES

Os métodos de ataque materializam (concretizam) a acção ou conjunto de acções utilizadas por uma ameaça (têm potencial) para explorar uma ou mais vulnerabilidades de um determinado activo dos SI organizacionais, consequentemente na dissertação diferenciamos ameaça de método de ataque.

Relativamente aos métodos de ataque utilizados pelas ameaças, para atacarem as infra-estruturas e os sistemas de Comando e Controlo (ou seja os seus SI de suporte) utilizamos a tipologia do FM 3 – 13 (2003), mantendo a coerência conceptual com a tipologia das ameaças, que classificamos da seguinte forma:

- Forçar o acesso não autorizado – com o intuito de obter informação, alterar, modificar ou mesmo apagar informação de sistemas de informação e dos sistemas de C2. As redes militares (redes informáticas em geral), por usarem muitas das infra-estruturas públicas, podem ser acedidas a partir da Internet.

- Projecção de software malicioso – tem em vista fazer com que o computador funcione de forma diferente da esperada, e pode incluir vírus, *worms*, ou seja "armas digitais" em sentido lato. O acesso à Internet, sobretudo pelo *download* de software, pode abrir as portas a software malicioso que pode, por sua vez destruir informação ou mesmo permitir o acesso aos sistemas amigos.

[12] O Exercício "*O Dia Seguinte ... no Ciberespaço*" surge na sequência do conjunto de matérias ministradas no âmbito da disciplina de Guerra de Informação, da Pós-Graduação em GICI da Academia Militar, procurando constituir o corolário do seu processo pedagógico. A metodologia do exercício "The Day After..." tem vindo a ser desenvolvida em diversos Países (EUA, Reino Unido, França, Alemanha), com o objectivo de explorar as implicações da evolução do ambiente estratégico internacional pós-Guerra Fria na Segurança e Defesa Nacional, em especial no que se refere às implicações estratégicas do terrorismo multinacional e dos novos tipos de guerra (incluindo a Guerra de Informação). A preparação e planeamento do Exercício "O Dia Seguinte ... no Ciberespaço", teve por base o Exercício "The Day After... in Cyberspace - II", conduzido pela *Advanced Research Projects Agency (ARPA)*, em 23 de Março de 1996.

• Decepção electrónica – consiste na emissão de energia electromagnética com vista a manipular, simular ou imitar comportamentos que enganem o adversário.

• Ataque electrónico – consiste no uso de energia electromagnética com vista a degradar, neutralizar ou destruir a capacidade de combate adversária. É considerada uma forma de fogos. Inclui lasers, armas de radiofrequência e feixes de partículas.

• O Ataque a Redes de Computadores - é uma outra forma de ataque que pode ser também levado a cabo. As redes de computadores são particularmente vulneráveis a ataques de negação de serviço (DoS), os quais, mesmo sem que se chegue a ganhar acesso à rede a tornam inoperacional.

• Destruição física – Como o próprio nome indica, consiste na destruição física, por meios físicos ou electrónicos do alvo.

• Gestão das Percepções – acções que visam influenciar audiências específicas, nas quais são usadas combinações das outras capacidades de forma coordenada (operações psicológicas, propaganda, decepção), que visam minar a vontade do adversário.

Nos métodos de ataque mais focados em tecnologia (projecção de software malicioso e no ataque a redes de computadores), complementamos com a classificação proposta por Kurose e Ross (2008) e que consiste na seguinte taxionomia:

- Utilização de *Malware* (ex. *Virus, worms e trojans*).
- *Denial of service* (DoS).
- *Packet Sniffer*.
- *Masquerade (ex. IP spoofing*).
- Modificar e apagar mensagens (*man-in-the-middle*).

ARMAS

Algumas das ameaças referenciadas podem utilizar um possível conjunto de "armas" nos seus diversos métodos de ataque descritos, que permitem explorar as vulnerabilidades existentes nos SI de uma organização.

Podemos face aos métodos de ataque descritos considerar a utilização de armas de destruição física sobre nós de comunicações e sistemas de informação, a título de exemplo; de armas de sintaxe (ex. vírus), tendo como objectivo atacar a lógica operacional de um sistema de informação através da introdução de atrasos ou comportamentos imprevisíveis no seu funcionamento ou ainda adquirindo o seu controlo, desactivando-o e de armas de semântica, que têm como objectivo a destruição ou afectação da confiança que os utilizadores depositam tanto nos recursos de informação como nos vectores que os transportam (manipulação, modificação ou destruição dos modelos de apoio à decisão, afectando a percepção e a representação da realidade) (Nunes, 1999).

CONCLUSÃO

As dimensões de segurança sugeridas pretendem barrar os principais eixos para as ameaças à organização aplicarem os seus possíveis métodos de ataque (visão *Top - Down*). A perspectiva militar das Operações de Informação e os métodos de ataque apresentados, bem como os componentes dos Sistemas de Informação, indicam as possíveis dimensões de segurança da informação a considerar.

Simultaneamente procuraremos numa aproximação *Bottom-Top*, utilizando a metodologia de análise de vulnerabilidades de um SI sugerida na Figura 5, obter os seus principais componentes e indicadores da Segurança da Informação, de acordo com os diferentes controlos obtidos da revisão bibliográfica, ajustando-os por critérios de funcionalidades de administração e semelhanças técnicas às dimensões de segurança obtidas.

3.2 DIMENSÕES DA SEGURANÇA

A Guerra de Informação suportada em Operações de Informação pode afectar o SI de uma organização, atingindo na essência a segurança da informação. 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 nas TI.

No contexto Militar apresentado, consideramos o SI[13], segundo a doutrina militar Americana, como " *a infra-estrutura completa, organização, pessoal e componentes que recolhem, processam, armazenam, transmitem, mostram, disseminam e actuam na informação*" (FM 100-6, 1996, 5-0), cuja definição perspectiva consequentemente as dimensões a considerar para a segurança da informação.

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 da organização militar, teve por base duas abordagens distintas, com base em critérios de operacionalização e gestão:

- Considerarmos uma abordagem *Top-Down* para 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 (visão militar de defesa face ao inimigo) e tendo como aspecto crítico garantir a continuidade do negócio da organização (o cumprimento da missão).

[13] Esta definição suportou a obtenção das dimensões da segurança da informação representadas na Framework, de acordo com as seguintes ligações: Organização / ***Organização & Planeamento***; Infra-estrutura / ***Física***; Pessoal / ***Pessoal*** e Componentes / ***Tecnologia*** (Aplicacional, Redes e Lógica).

- Face no entanto à extensa literatura técnica existente sobre controlos a implementar para garantir a segurança da informação realizamos simultaneamente uma abordagem *Bottom-Top*, em que procuramos agrupar os indicadores por funcionalidades de administração e semelhanças técnicas.

Na selecção dos indicadores procuramos considerar como critérios de validação:

- A existência de justificação para a sua necessidade ou seja é necessário para garantir a defesa do componente, resultando cada indicador numa possível lista de verificação;
- É específico, mensurável, alcançável dentro de um período de tempo aceitável e é realista a sua implementação.
- Leva à criação de procedimentos ou instruções de trabalho para resolver ou limitar o problema e à necessidade de atribuir responsabilidades de controlo.

Face à abrangência das dimensões e componentes, os indicadores são resultado de uma avaliação qualitativa decorrente da observação, aos quais futuramente poderão estar associadas listas de verificação. Estes na sua maioria estão alinhados com as boas práticas e controlos de segurança referidos nas diversas Frameworks de Segurança de SI e metodologias de identificação e avaliação de riscos para a segurança dos SI, indicadas na revisão bibliográfica.

Face à complexidade técnica e abrangência das dimensões associada à limitação temporal, validamos apenas alguns dos seus componentes, considerando estes como os *Drives* principais de suporte de cada dimensão da segurança, de forma a obter uma "imagem" integral de um possível modelo conceptual de Gestão da Segurança da Informação.

DIMENSÃO ORGANIZACIONAL

Esta dimensão tem como finalidade efectuar a análise da organização, da 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[14]. É fundamental a correcta visão geral da organização, de modo a garantir o correcto planeamento e implementação da Framework de Segurança.

[14] Conforme é referido na ISO/IEC 17799 (2005).

Identificamos na Tabela 1 o que pensamos serem os seus principais componentes e indicadores, tendo como principais preocupações conhecer as reais e potenciais ameaças à organização e os activos críticos a proteger.

DIMENSÃO	COMPONENTES	INDICADORES (prováveis)
ORGANIZACIONAL	1. Sistema de Gestão de Qualidade	Missão, politica e visão
		Requisitos de negócio
		Processos de negócio
		Gestores de Processos
	2. Sistemas de Informação	Áreas operacionais e actividades
		Gestão de serviços de TI
		Gestores operacionais
		Especialistas
		Falhas na análise e desenho do SI
	3. Interfaces	Cadeia de valor
		Sub-sistemas
		Intercâmbios de informação
	4.Legislação e Normas	Nacionais e internacionais
		Requisitos legais para as TI
		Requisitos de clientes (internos e externos)
		Estrutura ética
	5. Sistemas de Gestão	*Capacity Planning*
		Gestão de Projectos
		Gestão da Mudança
		Gestão do Conhecimento
		Gestores de projectos
	6. Análise Estratégica	Análise SWOT
		Análise das cinco forças de Porter
		Identificação e análise de ameaças
	7. Infra-estrutura de Segurança	Comité de segurança (planear e aprovar)
		Comité de gestão (coordenar a implementação)
		Responsáveis dos processos /activos (executar)
	8. Outros	…

Tabela 1 – Dimensão Organizacional da Segurança da Informação

Consideramos como um dos seus componentes o Sistema de Gestão de Qualidade, suportado numa abordagem por processos. Para que uma organização funcione de forma eficaz, necessita de identificar e gerir numerosas actividades interligadas, sendo uma decisão estratégica da organização (ISO 9001, 2001). Tomamos por referência a ISO 9001 e a análise dos processos do IGeoE, como organismo certificado no sistema integrado de Gestão de Qualidade e Ambiente segundo as normas NP EN ISO 9001 (2000) e NP EN ISO 14001 (1999).

Uma actividade utilizando recursos e gerida de forma a permitir a transformação de *inputs* em *outputs*, pode ser considerada um processo, sendo frequente a saída de um processo constituir directamente a entrada de outro. Na abordagem por processos uma das vantagens é a melhoria dos processos baseada na medição dos objectivos.

Neste componente efectuamos o levantamento de processos e analisamos a sua gestão operacional, os fluxos de informação, as tecnologias de suporte e as pessoas envolvidas em cada um dos processos, numa perspectiva de segurança da informação, obtendo após consulta dos gestores dos processos uma indicação dos principais activos críticos a proteger de acordo com a missão da organização.

Nos Sistemas de Informação, procuramos identificar nas áreas operacionais e suas actividades, a tecnologia de suporte (ex. *hardware*, *software)*, controlos de segurança implementados e vulnerabilidades. Analisamos simultaneamente a gestão de serviços de TI, utilizando a filosofia ITIL, que adopta uma abordagem orientada por processos e que podemos escalonar de modo a adaptar a grandes e pequenas empresas. Devemos ter a preocupação da ligação com a dimensão física pelos possíveis meios de acesso físico às tecnologias de suporte e à dimensão pessoal devido à importância cada vez maior dos especialistas que a suportam.

A gestão de Serviços de TI segundo a abordagem ITIL, analisa os processos que precisam de ser realizados dentro da organização para a gestão e operação das infra-estruturas de TI, para promover um serviço óptimo para o cliente a custos justos, no qual se inclui a segurança da informação.

Com o componente Interfaces procuramos identificar e analisar os sistemas que interagem com a nossa organização (ex. clientes, fornecedores e entidades reguladoras) através da sua cadeia de valores, especialmente através dos fluxos de informação. Neste componente é essencial definir as fronteiras do nosso sistema.

Na Legislação e Normas, identificamos a regulamentação jurídica das actividades de uma organização, integrando os requisitos dos clientes, a utilização das TI, ao mesmo tempo que analisamos a estrutura ética da organização em termos de privacidade, propriedade e acessibilidade.

Os Sistemas de Gestão, apresentam na nossa perspectiva, processos de gestão “especiais”, na medida em que não reflectem a gestão operacional, mas sim uma gestão estratégica com implicações na sobrevivência da empresa a médio e longo prazo.

A organização deve possuir planos de evolução tecnológica e de negócio, que na realidade serão a alavanca de novos projectos, suportados em modelos de gestão da mudança e garantindo a gestão do seu conhecimento, nos quais devemos procurar ter sempre e desde início uma preocupação com a segurança da informação.

A componente Análise Estratégica procura através de metodologias conhecidas identificar as forças e fraquezas da organização a nível interno, ao mesmo tempo que identifica as suas ameaças e oportunidades externas através de uma análise *SWOT*. Pode e deve detalhar com mais profundidade os seus concorrentes reais, potenciais e substitutos, seus clientes e fornecedores, através do modelo das cinco forças concorrenciais de *Porter*.

A Infra-estrutura de segurança indica as entidades responsáveis por planear, aprovar, coordenar, implementar e garantir a segurança da informação na organização.

Figura 15 – Dimensão Organizacional da Segurança da Informação

Em conclusão, consideramos na dimensão organizacional como componentes principais a analisar e considerar para a eficaz implementação de um Sistema de Gestão da Segurança da Informação os indicados na Figura 15. A componente Análise Estratégica é considerada por nós a principal *drive* da dimensão, pela importância para toda a metodologia de aplicação, da correcta identificação e análise de ameaças. Esta identificação de ameaças permitirá com rigor e detalhe cenarizar possíveis ataques para exploração das vulnerabilidades dos activos críticos identificados nos SI organizacionais.

DIMENSÃO PLANEAMENTO

Esta dimensão integra o planeamento e a gestão de todos os controlos (indicadores) da segurança da informação, considerando todos os recursos de suporte e medidas implementadas para garantir a sua segurança nas diferentes dimensões apresentadas na *Framework.*

Na Dimensão Planeamento, identificamos na Tabela 2, o que pensamos serem os seus principais componentes e indicadores. A componente Identificação e Avaliação de Riscos apresenta a prioritização dos riscos do SI já identificados pela organização ou devido à sua inexistência procuramos aplicar uma metodologia de referência de forma a apresentar ao decisor uma imagem clara dos riscos à segurança dos SI.

Um outro componente é a Política de Segurança como documento estruturante da gestão da segurança dos SI e consequentemente da informação. A sua ligação à identificação e avaliação do risco e sua gestão integrada, permite-nos suportar a implementação e gestão actual e futura dos controlos de segurança ao nível dos diversos domínios apresentados.

As Políticas, Normas e Procedimentos de Segurança integram os principais indicadores de planeamento que reflectem as boas práticas de segurança dos SI organizacionais. Esta componente assume o papel de *drive* principal nesta dimensão em virtude da análise dos seus indicadores permitir ter a percepção imediata dos controlos planeados e implementados a nível da organização.

Podemos definir as Políticas como um conjunto reduzido de regras que definem em linhas gerais, o que é considerado pela organização como aceitável ou inaceitável, contendo ainda referências às medidas a impor aos infractores. As Normas são o documento composto por todas as regras de segurança da empresa, concretizando em detalhe as linhas orientadoras estabelecidas na Política de segurança e um Procedimento é um documento que descreve uma operação de forma muito detalhada, ou seja, indicando todos os seus passos (Silva et al, 2003, p. 181).

DIMENSÃO	COMPONENTES	INDICADORES (prováveis)
PLANEAMENTO[15]	1.Identificação e Avaliação de Riscos	Metodologia de referência
		Relatório classificado
		Inventário de activos (inclui a informação)
	2.Política de Segurança	Documento
		Publicada e comunicada
		Revisões assinaladas
	3.Políticas, Normas e Procedimentos de Segurança	Politica de recursos humanos
		Normas de segurança (assinadas, só o necessário)
		Classificação e gestão da informação
		Procedimentos de uso de *passwords*
		Procedimentos de uso de equipamentos
		Procedimentos de uso de meios de armazenagem
		Procedimentos de acesso à internet
		Procedimentos de uso do correio electrónico
		Política de gestão de continuidade
		Política de controlo de acessos integrada
		Política de comunicação /difusão de informação
		Política de cópias de segurança
		Política de retenção de logs
		Política de "mesa/tela" limpa
		Política de computação móvel
		Política de uso de software
		Política de aquisições
	4. Plano Global de Segurança	Objectivos
		Situação actual
		A estratégia
		Plano de acção
		Benefícios
		A estrutura funcional da equipa
		Orçamento e recursos necessários
		Terminologia técnica
	5.Auditorias de Segurança	Relatórios internos e externos
		Testes de intrusão (ex. cenarização de ataques)
		Detecção de vulnerabilidades e correcção automática
	6.Monitorização, Detecção e Resposta a Ataques	Relatórios de incidentes
		Medidas dissuasivas (dificultam os ataques)
		Medidas de detecção (descobrem os ataques)
		Medidas de diversão (iludem os ataques)
		Entidades a contactarem (ex. CERT)
	7.Continuidade do Negócio	Plano de disaster recover (com suporte na IAR)
		Cenários identificados e analisados de risco
		Arquitectura de disaster recover
		Site alternativo
		Equipa de recuperação
		Ensaios dos planos
		Relação com a ITSM (ITIL)
		Formação específica
		Manutenção e revisão do plano
	8.Delitos e Análise Forense	Entidade responsável
		Procedimentos para obtenção da prova
		Relatórios
		Consequências criminais e disciplinares
	9. Outros	…

Tabela 2 – Dimensão Planeamento da Segurança da Informação

[15] Têm como referência principal a ISO / IEC 27001 (2005).

O Plano Global de Segurança espelha o estado de segurança organizacional, a sua visão estratégica e intenção futura para garantir a segurança da informação, com base em planos de acção de forma a implementar os controlos planeados.

As Auditorias de Segurança internas ou externas como medida de detecção, permite-nos avaliar a eficácia das medidas de segurança planeadas e executadas, (ex. aplicando testes de intrusão) e garantindo as suas correcções.

A componente Monitorização, Detecção e Resposta a Ataques garante a vigilância dos indicadores da segurança dos SI e da funcionalidade do sistema como um todo, procurando introduzir e verificar a eficácia das medidas dissuasivas, de detecção e de diversão. Neste componente é essencial a criação de uma equipa de resposta a incidentes de segurança, do qual é fundamental o componente de segurança informática, designado tradicionalmente a nível internacional pela sigla CERT (*Computer Emergency Response Team*) e mais recentemente pela CSIRT (*Computer Security Incident Response Team (s)*).

Para evitar a disrupção de funcionamento da organização após um ataque, temos que ter especial atenção à existência e à operacionalização dos planos de *Disaster Recover* garantindo a Continuidade do Negócio[16] e consequentemente a sobrevivência da organização. Este componente é uma das principais medidas que possibilitam reduzir o impacto de um ataque ao SI. Sendo o papel principal na sobrevivência da organização a garantia de funcionamento dos seus Centros de Processamento de Dados.

Numa visão menos "agressiva", pode-se referir o ataque como um desastre. Sendo este definido como qualquer evento que atinja os SI de uma organização de forma súbita, interrompendo um serviço vital ou corrompa os dados, negue o acesso à informação ou inviabilize os SI (Serrano e Jardim, 2007). Face à probabilidade de ocorrência de um desastre é necessário avaliar a necessidade de implementar uma solução de *Disaster Recover*, tendo no entanto que pesar alguns factores, dos quais salientamos: a identificação e avaliação do risco, o impacto causado pela sua ocorrência, a sua probabilidade e o período máximo que uma organização se consegue manter indisponível (Serrano e Jardim, 2007).

[16] Uma das certificações disponíveis no mercado é a *Certified Business Continuity Professional* que é emitida pelo *Disaster Recovery Institute International* com sede em St. Louis, Missouri ou a BS 25999 – 1: 2006.

Sendo a análise das evidências de um ataque efectuada através da componente Delitos e Análise Forense**,** devemos garantir o cumprimento dos procedimentos correctos para a obtenção da prova, alertando a entidade responsável e difundindo de antemão as consequências criminais e disciplinares para os colaboradores internos ou em *outsourcing.* Este componente visa garantir que na evidência[17] digital (indício) obtida, nenhum dado possa ser adicionado ou removido, exigindo consequentemente elevada capacidade técnica e científica da entidade que efectua a obtenção da prova, de forma a suportar legalmente a acusação (Marcella e Greenfield, 2002).

Exige que existam procedimentos testados, que garantam que após os ataques efectuados através de computadores, os métodos utilizados na obtenção das provas não alterem os indícios. É fundamental que os aspectos técnicos sejam guiados pelos de ordem legal, garantindo deste modo que os procedimentos periciais sejam sustentáveis em juízo.

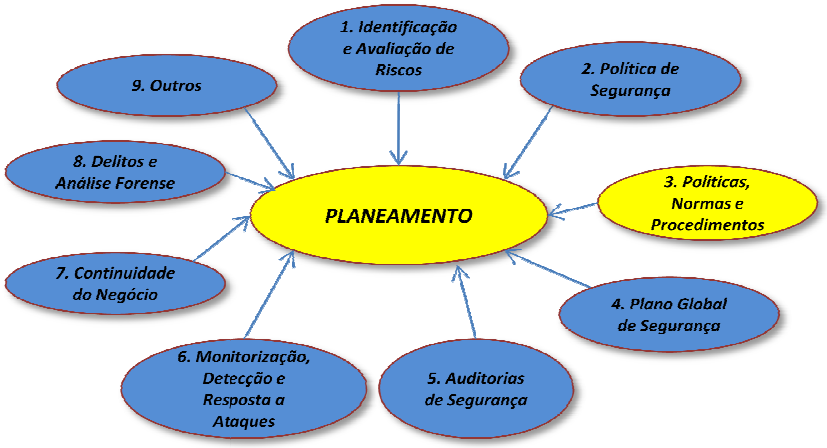


Figura 16 – Dimensão Planeamento da Segurança da Informação

A dimensão planeamento tem fundamentalmente como referenciais as normas ISO / IEC 27001 (2005) e a ISO / IEC 17779 (2005) (actualmente ISO/IEC 27002), como diagnóstico de boas práticas de segurança da informação em 10 áreas chave.

Em conclusão, a componente Políticas, Normas e Procedimentos de Segurança é por nós considerada a principal *drive* da dimensão, reflectindo a identificação e avaliação de riscos em segurança da informação, que anteriormente foi realizada pela organização e devendo garantir-se a centralização toda a documentação produzida.

[17] É o vestígio (ex. material) que após ser devidamente analisado e interpretado, estabelece a relação inequívoca com o facto de delito e as pessoas com ele relacionadas.

DIMENSÃO FÍSICA

Na dimensão física, consideramos fundamentalmente os componentes e indicadores assinalados na Tabela 3, tendo como principal objectivo garantir a protecção física dos SI no global e de todos os seus componentes (hardware, software, documentação e meios magnéticos) no particular. Esta protecção considera principalmente os riscos por roubo, extravios ou por danos físicos (Carneiro, 2002).

No componente Emergência Interna consideramos o seu plano hoje reconhecido como uma ferramenta eficaz, que se bem aplicada, dará um importante contributo para a redução de riscos na organização. A perspectiva de análise deste documento operacional, é obter os indicadores que visem prevenir a ocorrência dos acontecimentos graves e estabelecer um conjunto de procedimentos que viabilizam uma resposta eficaz caso aqueles ocorram, fundamentalmente na perspectiva da sua segurança física.

No componente Infra-estrutura Crítica, analisamos os sistemas cuja ruptura pode produzir efeitos de âmbito nacional, ou regional de tal forma que afecte o regular funcionamento dos sistemas de informação da nossa organização.

Nas Instalações da organização, deve procurar-se efectuar uma análise cuidadosa às suas plantas originais (ex. estrutura, energia eléctrica e cablagem), aos seus pontos de acesso exteriores, à informação e aos equipamentos de suporte existentes em cada área. Devemos fazer corresponder a cada área uma classificação de segurança (ex. classes de áreas de segurança[18]) e integrar com a credenciação do pessoal que acede fisicamente ou remotamente a essa informação.

Nos Equipamentos, devemos considerar a identificação e manutenção dos que contactam ou suportam a informação, bem como a existência de uma entidade responsável pela sua segurança. No hardware (ex. computadores, impressoras), é essencial analisar a sua disposição e protecção física, tipos de manutenção realizada (ex. preventiva, correctiva), garantindo simultaneamente as evidências das mudanças de localização internas e externas efectuadas.

[18] Podemos referir a título de exemplo a classificação apresentada no SEGNAC 2 para as áreas de segurança (1989, p. 4676).

DIMENSÃO	COMPONENTES	**Prováveis Indicadores** (nível de exposição)	Ex. Ameaças x Métodos de Ataque
FÍSICA[19]	1. Emergência Interna[20]	Plano de emergência interna	Desastres naturais.
			Espionagem e sabotagem.
		Detecção e combate a incêndio	Incêndio/explosão
		Detecção e combate a inundação	Inundação
		Detecção de fuga de gás	Fuga de gás
		Protecção de pontos perigosos	Origem de acidentes
	2.Infra – Estrutura Crítica	Rede eléctrica (alternativa e segurança)	Falha da energia eléctrica
		Telecomunicações (alternativa e segurança)	Falha nos sistemas comunicação
	3.Instalações	Plantas da organização	- Intrusão e roubo; - Acesso indevido.
		Tipos de acessos controlados	
		Classificação de áreas[21]	
		Estrutura física	
	4.Equipamentos	Catálogo de equipamentos (HW)	- Intrusão e roubo; - Acesso indevido; - Campo magnético; - Impacto mecânico; - Decomposição química; - Calor; - Poeira; - Radiações emanadas.
		Catálogo de meios armazenamento	
		Identificação dos equipamentos	
		Responsáveis	
		Tipo de acesso	
		Disposição e protecção física	
		Pontos de acesso à rede	
		Registo de movimentos manutenção	
	5.Áreas Críticas[22]	Localização	- Intrusão e roubo; - Acesso indevido; - Uso de meios físicos para explorar vulnerabilidades estruturais.
		Classificação	
		Estrutura (ex piso, tecto e paredes)	
		Iluminação e indicações visuais	
		Organização e limpeza	
		Energia eléctrica (UPS)	
		Geradores de suporte	
		Sistemas de vigilância	
		Cablagem	
		Climatização (AVAC)	
		Controlo de acesso	
		Detecção e combate a incêndios	
		Monitorização	
		Procedimentos de emergência	
		Ligação terra local	
		Detecção e escoamento inundações	
	6.Controlo de Acessos	Perímetro de segurança física	- Forçar o acesso não autorizado; Intrusão e roubo; Acesso indevido.
		Sistemas de vídeo vigilância	
		Sistemas de alarmes	
		Pontos de acesso	
		Sistemas de controlo e registo	
	7. Eliminação / Reutilização	Equipamentos e documentação	*"Dumpster diving"* (analise lixo).
	8.Protecção de Escutas, Observação e Radiações Electromagnéticas	Insonorização	Escuta activa e passiva
		Especificações *"Tempest"*	Ataque electrónico e decepção
	9.Manutenção e Assistência Técnica	Interna e externa	- Acesso indevido; - Deterioração.
		Relatórios	
		Contractos de manutenção	
	10. Outros	…	…

Tabela 3 – Dimensão Física da Segurança da Informação

[19] Referido em SEGNAC 1 (1988), SEGNAC 2 (1989), ISO/IEC TR 13335-4 (2000), Oliveira (2001), Wadlow (2001), Carneiro (2002), RAD 280-1 (2003), Silva et al (2003), ISO 17799 (2005) e Modelo de Segurança da NATO.

[20] Têm por referência a OHSAS 18001:1999, o plano de emergência interna do IGeoE e o SEGNAC 2 (1989, p.4683). O IGeoE é certificado segundo o referencial OHSAS 18001:1999 (NP 4397:2001) (Sistemas de Gestão da Segurança e Saúde no Trabalho).

[21] Ao nível NATO, consideram-se áreas de Classe 1, 2 e zonas administrativas (AC/35-D/2001, 2002, p. 1-3)

[22] Têm por referência o SEGNAC 1 (1988), as boas práticas de construção de um centro de processamento de dados (d*atacenter*) e validado com a "auditoria" ao Centro de Dados do Ministério da Defesa Nacional.

No componente Áreas Críticas é fundamental a análise dos sistemas implementados nos locais onde se localiza a informação crítica ou que com ela interagem. Devem ser prioritariamente considerados os centros de processamento de dados, a sala de armazenagem das cópias de segurança da informação e as salas de reuniões.

O componente Controlo de Acessos, visa impedir os acessos físicos não autorizados aos SI, garantindo a execução dos procedimentos implementados. Este deve garantir a primeira barreira de controlo de acessos, sendo a segunda através da identificação e autenticação no terminal e a terceira pelo controlo no acesso à informação devido à sua classificação. Devemos ter em consideração simultaneamente o controlo de todos os objectos transportados pela entidade (ex. portáteis, telemóvel e pen´s).

A gestão dos sistemas de controlo de acessos é efectuado por pessoas e consequentemente a sua credenciação deve estar de acordo com a criticidade da tarefa. A informação existente nas diversas áreas deve regular para além da classificação da área, a credenciação das pessoas que a ela têm acesso directa ou indirectamente (ex. acesso remoto).

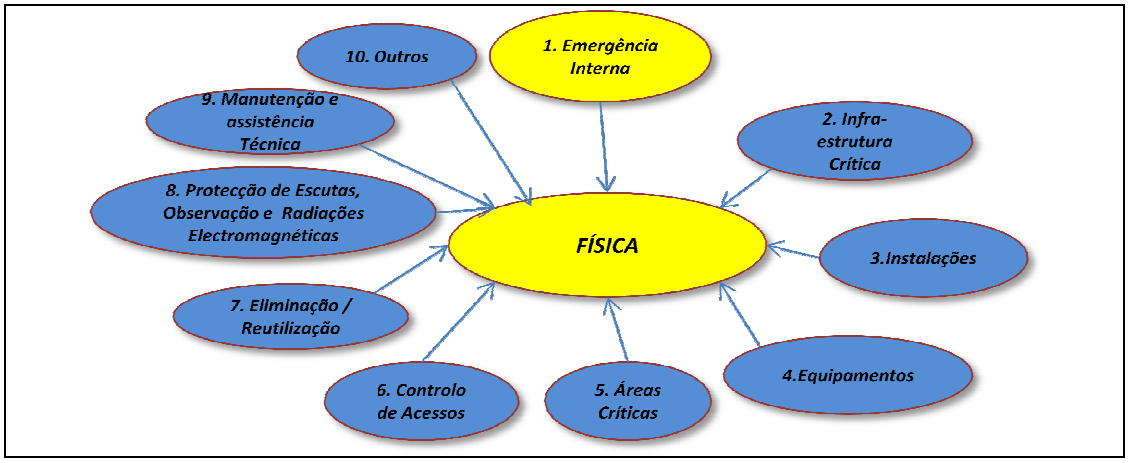


Figura 17 – Dimensão Física da Segurança da Informação

Garantir que os documentos, equipamentos ou meios de armazenagem destruídos ou reutilizados não permitam a recuperação de informação por elementos estranhos à organização, tendo especial atenção ao material depositado nos caixotes do lixo (ex. papeis e CD / DVD) e à manutenção de equipamentos realizada em instalações exteriores à organização.

Deverão ser tomadas medidas tal como indicado no SEGNAC 1 (1988) quando julgado necessário, tanto durante o dia como de noite, para proteger a informação classificada que corra o risco de ser Observada (ex. monitores e documentos classificados em cima da secretária ou de fácil acesso), o mesmo deve ser considerado para possíveis acções de Escuta passiva e activa e evitar a possível captação da emissão de Radiação Electromagnética.

A escuta passiva visa obter informações classificadas através de meios de telecomunicações não protegidos ou por escuta directa, enquanto a activa usa microfones, com ou sem fio, ou outros dispositivos instalados para o mesmo efeito.

Na componente Manutenção e Assistência Técnica**,** devemos internamente criar memorandos de entendimento com as entidades que prestam os serviços e na externa pela existência de *Service Level Agreements* (SLA) com as entidades que executam o *outsourcing*.

Em conclusão**,** na Dimensão Física consideramos como componentes principais a analisar e considerar para a eficaz implementação de um Sistema de Gestão da Segurança da Informação os indicados na Figura 17.

Consideramos o componente Emergência Interna como *drive* principal desta dimensão, em virtude de após identificarmos e analisarmos as ameaças podermos neste componente identificar as principais vulnerabilidades físicas que podem ser exploradas na organização e simultaneamente por o plano de emergência interna ser um dos principais planos de segurança aplicados na organização militar.

DIMENSÃO PESSOAL

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 (Alexandre, 2005).

No componente Recrutamento e Saída é necessário garantir a idoneidade dos colaboradores, efectuando a verificação dos seus dados, credenciando-os para o manuseamento dos dados e informação a que terão acesso, apresentando-lhe a filosofia de segurança da organização e garantindo a sua aceitação. O recrutamento interno ou externo consiste num conjunto de procedimentos com o objectivo de atrair candidatos potencialmente qualificados e capazes de ocupar cargos dentro da organização (Chiavenato, 1989). Na sua saída voluntária ou involuntária, devemos garantir procedimentos de recolha de todos os recursos da organização na sua posse (ex. portátil), bem como garantir a desactivação de todas as suas formas de identificação e autenticação em sistemas da organização (ex. desactivar a conta no domínio e alterar *passwords* de acesso a recursos).

O componente Desempenho de Funções (ou Selecção) apresenta-se nesta dimensão como o seu *drive* principal, em virtude de reflectir as necessidades de competências para o desempenho de funções, em comparação com os perfis de competências actuais dos colaboradores, permitindo deste modo dar indicações precisas sobre as vulnerabilidades dos colaboradores que podem ser exploradas.

DIMENSÃO	**COMPONENTES**	**Prováveis Indicadores** (nível de exposição)	Ex. Ameaças x Métodos de Ataque
PESSOAL[23]	1.Recrutamento e Saída	Filosofia de segurança	Forçar o acesso não autorizado usando uma falsa entidade.
		Contrato de confidencialidade	
		"Background Check"	
		Procedimentos de saída	
		Procedimentos de demissão	
	2.Desempenho de Funções	Credenciação	- Acesso indevido; - Má utilização por desconhecimento, possibilitando métodos de ataque mais focados na tecnologia.
		Perfil do posto e do colaborador	
		Acesso de terceiros (outsourcing)	
		Registo de pessoal	
	3.Formação	Interna e externa	Formação deficiente, permitindo a sua manipulação.
		Acções de sensibilização	
	4.Engenharia Social (ES)	Metodologia de Referência	- Gestão de percepções; - Manipulação dos utilizadores; - Tipologia de ataques de ES; - Explorar lista vulnerabilidade *wetware* (pessoas).
		Boas práticas	
	5. Outros	…	…

Tabela 4 – Dimensão Pessoal da Segurança da Informação

[23] Referido em SEGNAC 1 (1988), ISO/IEC 13335:4 (2000), Wadlow (2001), Silva et al (2003), RAD 280-1 (2003), ISO 17799 (2005) e Modelo de Segurança da NATO.

A componente Formação é essencial para reduzir ou eliminar as vulnerabilidades identificadas no componente de desempenho de funções. Esta deve ser permanente e ajustada às funções do colaborador, procurando evitar os ataques de Engenharia Social. Internamente a organização deve desenvolver acções de sensibilização para as questões da segurança da informação (ex. relatar incidentes de segurança e alertar para vulnerabilidades e mau funcionamento de software), procurando desta forma e associado a outras formas de divulgação (ex. *intranets e newsletters*), alertar e simultaneamente realizar a gestão do conhecimento referente a esta temática.

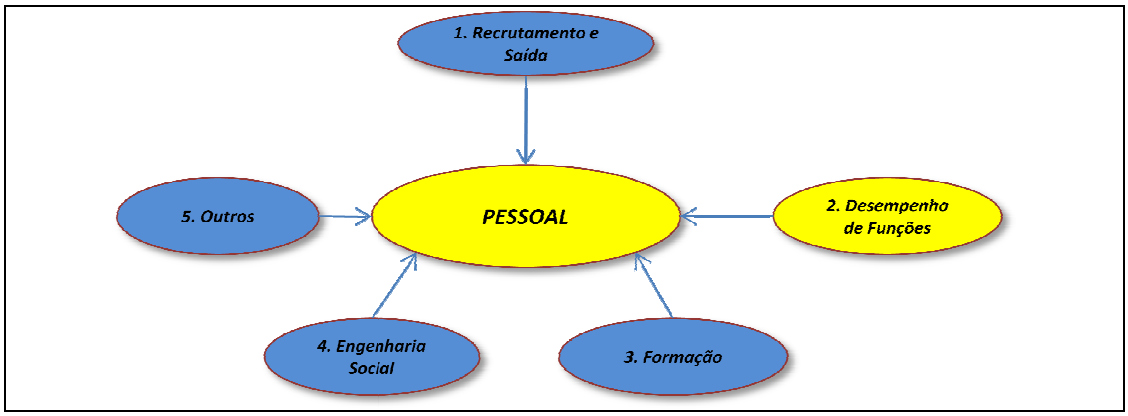


Figura 18 – Dimensão Pessoal

Na componente Engenharia Social, procuramos negar a obtenção de informações (*intelligence*) pelo adversário. Os ataques de engenharia social, baseiam-se principalmente em vulnerabilidades humanas (Mitnick e Simon, 2003) e tal como refere Alexandre (2005, p.1) " […] embora alguns conhecimentos técnicos possam também ser utilizados, a abordagem sob o ponto de vista da psicologia social incorpora conhecimentos há muito utilizados nos domínios das operações psicológicas". Uma das possíveis soluções é a utilização de uma metodologia, que procure uma alteração comportamental do elemento humano, evitando a sua manipulação ou alteração da percepção para a realidade.

Em conclusão**,** consideramos fundamental o cumprimento da máxima "pessoa certa no lugar certo", tendo consequentemente como drive principal desta dimensão o componente desempenho de funções. Esta dimensão deve prevenir fundamentalmente ataques de Engenharia Social, evitando a manipulação dos utilizadores de forma a convencê-los a realizar determinadas acções que visam alterar as propriedades da segurança da informação.

DIMENSÃO TECNOLÓGICA

Esta dimensão tem como objectivos garantir o correcto processamento, transmissão e armazenagem dos dados e informação, indispensáveis para garantir a segurança da informação. Como modelo conceptual para facilidade de percepção do decisor, separamos esta dimensão em três: uma dimensão aplicacional (processamento), uma lógica (identificação e armazenamento) e finalmente uma dimensão rede (transmissão). Cada uma das dimensões mais orientada para um dos objectivos referidos, mas sem com isso querer isolar as dimensões.

DIMENSÃO APLICACIONAL

Na dimensão aplicacional exploramos fundamentalmente os componentes e indicadores assinalados na Tabela 5, que reflectem a preocupação com a aquisição ou desenvolvimento, implementação, manutenção e a correcta utilização do software instalado na organização, tendo especial atenção à separação dos ambientes de desenvolvimento, testes e produção de forma a impedir os riscos de segurança.

DIMENSÃO	COMPONENTES	**Prováveis Indicadores** (nível de exposição)	Ex. Ameaças x Métodos de Ataque
APLICACIONAL[24]	1.Utilização	Catálogo de software	- Erros humanos por má utilização, facilitando ataques centrados na tecnologia; - Acesso indevido.
		Distribuição por níveis de SI	
		Utilizadores responsáveis	
	2.Controlo e Manutenção	Licenciamento	- CNA; - Projecção de software malicioso; -Ataques às aplicações por exploração de vulnerabilidades ("Holes").
		Configurações	
		Alterações	
		Versões (Releases)	
		Incidentes e problemas	
		Outsourcing de aplicações (SLA)	
		Análise do código fonte	
	3. Aquisição e Desenvolvimento	Processo de desenvolvimento de software[25]	Exploração das: - Vulnerabilidades de concepção; - Vulnerabilidades na aquisição.
		Características da qualidade de software[26]	
		Requisitos de qualidade e testes de software[27]	
		Processo de ciclo de vida de software[28]	
	4. Outros	…	…

Tabela 5 – Dimensão Aplicacional da Segurança da Informação

[24] Referido por Silva et al (2003).
[25] Podemos ter como referência a ISO/IEC 15504 (SPICE) ou o *Capability Maturity Model Integration do Software Engeneering Institute da Carnegie Mellon University*, que permite definir o nível de maturidade de uma organização para o desenvolvimento do software.
[26] Conforme refere a ISO/IEC 9126 – 1: 2001.
[27] Conforme refere a ISO/IEC 12119.
[28] Conforme refere a ISO/IEC 12207.

A componente Utilização reflecte a preocupação com o correcto uso do software existente na organização, interligando-se com alguns dos componentes referenciados na dimensão pessoal (ex. formação) e considerando a necessidade da existência de utilizadores responsáveis pela sua gestão (ex. administradores). Pode servir de referência a certificação internacional ECDL, de competências nas TIC para os utilizadores, orientada para o mercado de trabalho, que atesta que o seu detentor possui as competências e conhecimentos que lhe permitem utilizar eficaz e produtivamente as principais aplicações informáticas utilizadas nos computadores.

A componente Controlo e Manutenção tem como referencial os processos de gestão de serviços de TI, podendo servir de referência a abordagem ITIL, cujos objectivos são principalmente alinhar os serviços de TI com as necessidades actuais e futuras da organização, melhorar a qualidade dos serviços de TI fornecidos e reduzir a longo prazo o custo inerente à disponibilização de Serviços.

Na Aquisição e Desenvolvimento a preocupação fundamental é evitar que as vulnerabilidades das aplicações possam ser exploradas pelas ameaças como resultado do desenvolvimento de aplicações efectuadas *ad-hoc* internamente, quer pelas adquiridas a nível externo e das quais a organização na maior parte das vezes não tem acesso ao seu código fonte. Sendo também fundamental o controlo dos possíveis *downloads* a efectuar pelos utilizadores a partir da Internet.

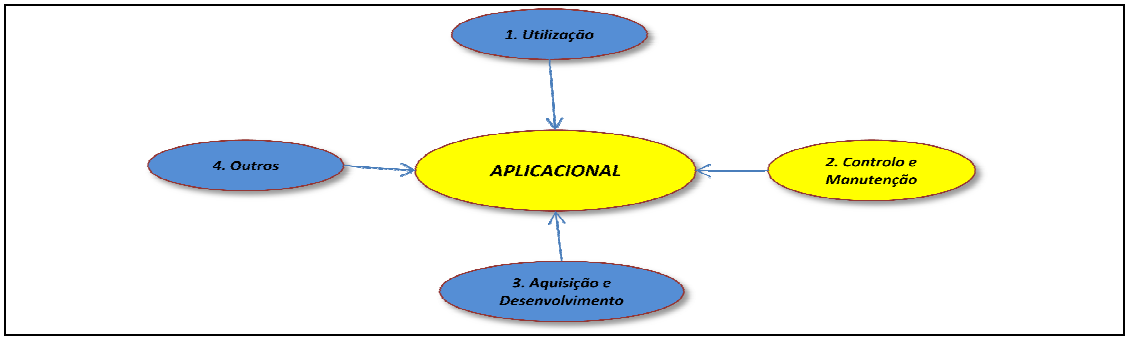


Figura 19 – Dimensão Aplicacional da Segurança da Informação

Em conclusão, consideramos nesta dimensão como *drive* principal o componente Controlo e Manutenção, sendo essencial que se reconheça a absoluta dependência da maioria das organizações da infra-estrutura das TIC e da quantidade, qualidade e disponibilidade das informações fornecidas e suportadas por esta infra-estrutura, daí a possível adopção do ITIL (MacFarlane e Rudd, 2003).

DIMENSÃO REDE

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.

DIMENSÃO	COMPONENTES	**Prováveis Indicadores** (nível de exposição)	Ex. Ameaças x Métodos de Ataque
REDE[29]	1.Servidores	Administradores	Má utilização por desconhecimento.
		Implementação de serviços	Explorar listas de vulnerabilidades.
		Configurações	Explorar listas de vulnerabilidades.
		Autenticação na rede	Acesso não autorizado.
		Sistemas operativos	Explorar listas de vulnerabilidades
	2.Clientes	Administradores	Má utilização por desconhecimento.
		Configurações	Explorar listas de vulnerabilidades.
		Clientes móveis	Explorar listas de vulnerabilidades.
		Autenticação na rede	Acesso não autorizado.
		Sistemas operativos	Explorar listas de vulnerabilidades.
		Uso de utilitários de sistema	
	3.Internet	Tipos de acesso e gestão	- Métodos de ataque (Expl. vulnerabilidades) • Perturbações de funcionamento, pela execução de software malicioso; • Negação de serviços; • Intercepção das comunicações; • Usurpação da identidade (Masquerade); • Modificar os dados em trânsito; • Acesso não autorizado (armas digitais)
		TCP/IP	
		Intranets e Extranets	
	4. Tecnologias de Segurança	Firewalls	
		Intrusion Detection Systems (ou IPS)	
		Antivírus	
		VPN	
		Criptografia e autenticação	
		File integrity checkers	
		Honeypots	
	5.Gestão da Rede	Tipo de rede (LAN, MAN, WAN)	Explorar listas de vulnerabilidades.
		Administradores	Má utilização por desconhecimento.
		Topologia da rede (ex. Ethernet)	Desconhecimento;
		Monitorização e gestão da rede	Má utilização por desconhecimento.
		Controlo de acesso à rede	Acesso não autorizado.
		Separação das redes	
	6.Activos	Implementação de serviços	Explorar listas de vulnerabilidades.
		Administradores	Má utilização por desconhecimento.
		Configurações	
		Protocolos de roteamento	
	7. Telecomunicações	Intercomunicadores	Explorar listas de vulnerabilidades.
		Telefones	
		Telemóveis	
		Fax	
	8. NAS ou SAN	Network attached storage (servidor)	Explorar listas de vulnerabilidades.
		Storage area network (rede)	
	9. Outros	…	…

Tabela 06 – Dimensão Rede da Segurança da Informação

Nos componentes Servidores e Clientes a preocupação principal prende-se com a sua eficiente administração, no efectuar as configurações correctas dos respectivos serviços que são necessários e na exploração eficaz em termos de segurança dos sistemas operativos em utilização. Os mesmos indicadores podem considerar-se como fundamentais para o componente Activos de rede (ex. *Routers e Switches*).

[29] Referido em ISO / IEC 13335-5 (2001), Wadlow (2001), Carneiro (2002), NIST 800-42 (2003), Silva et al (2003) e *INFOSEC (2004)*. A orientação teórica seguida é a apresentada por Tanenbaum (1997) e kurose e Ross (2008).

Um componente fundamental desta dimensão é a Internet, como interface tecnológica principal com os SI organizacionais, mas simultaneamente como meio principal de *Cyberwarfare*. Afirmamos que uma máquina pertence à Internet quando ela " […] executa a pilha de protocolos TCP/IP, têm um endereço IP e pode enviar pacotes IP a todas as outras máquinas da Internet " (Tanenbaum, 1997, p.79).

Tomamos por referência na dissertação essencialmente os seguintes tipos de acesso à Internet e as possíveis vulnerabilidades daí resultantes: o acesso *Dial-up*, o *Digital Subscrite Line* (DSL), o *Hybrid Fiber-Coaxial Cable* (HFC), a *LAN technology Ethernet* (IEEE 802.3) e o *Wireless Access* (IEEE 802.11). Na análise dos diversos *layers* do TCP-IP, devemos procurar identificar todas as possíveis aplicações em uso (*layer* 1), como possíveis pontos de entrada de *Maldware* (kurose e Ross, 2008).

Podemos obter e validar algumas das principais ameaças do ciberespaço, com base em Richardson (2007), pela análise dos dados obtidos de um inquérito realizado a 494 empresas de vários sectores nos Estados Unidos, para um dos actores principais das relações internacionais, os Estados Unidos da América.

Nesta dimensão consideramos como *drive* principal as Tecnologias de Segurança implementadas ou a implementar e nas quais devemos considerar fundamentalmente:

- 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, permitido 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, 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 consequentemente 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 IDS (chamados IPS).

- 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 Antivírus, 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 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 detiver uma chave que permita decifrá-la (Marques e Guedes, 1998). As técnicas para implementar canais de comunicação seguros podem subdividir-se em dois grandes grupos:

    - 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.

Na autenticação, o uso da assinatura digital é fundamental para assegurar a legitimidade da informação electrónica. O que queremos garantir é que o destinatário possa provar que o documento foi enviado por determinado agente.

- 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 *host.*

Na 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 titulo 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"* (NIST 800-42, 2003, p.3-1).

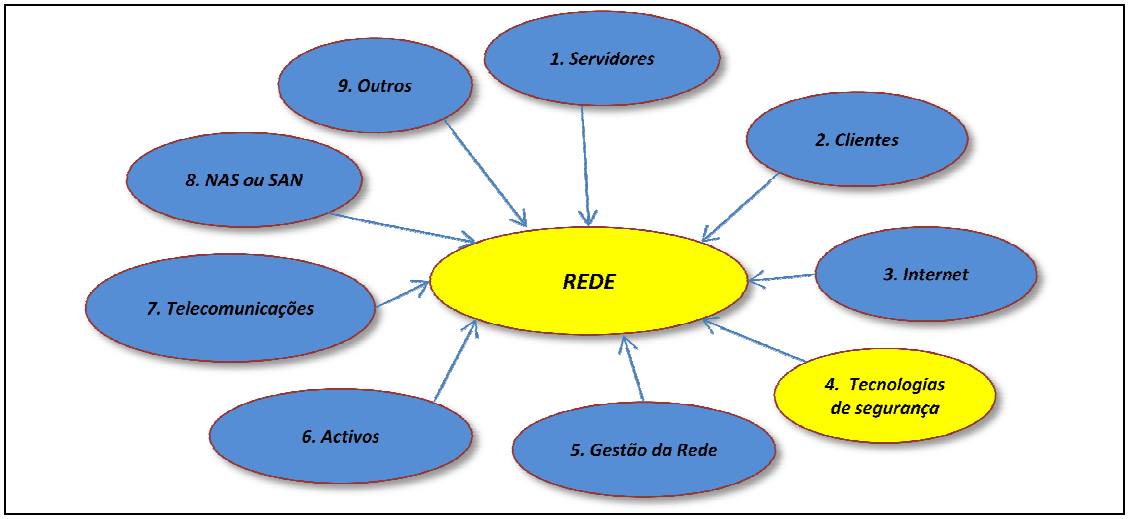


Figura 20 – Dimensão Rede da Segurança da Informação

Na Gestão da Rede é necessário efectuar a sua monitorização em tempo real de forma a garantir uma resposta imediata e eficaz a um incidente que possa ocorrer ou se preveja que ocorra face à comparação em cada instante dos indicadores de funcionamento da rede com a *baseline* de normal funcionamento. É necessário para isso possuir um software de apoio que permita efectuar toda a sua gestão de forma o mais simples e eficiente possível.

No componente Telecomunicações consideramos todas as outras tecnologias (ex. telemóveis) que permitem alterar fundamentalmente a propriedade *confidencialidade* da informação.

DIMENSÃO LÓGICA

Esta dimensão considera indispensável garantir o acesso autorizado dos utilizadores à informação e a sua correcta armazenagem e segurança. Para implementar uma política de controlo de acessos é necessário dispor de duas operações de base tal como refere Marques e Guedes (1998, p.249) "A Autenticação ou seja a operação de validação do agente e a Autorização, como operação que valida os direitos do agente sobre o objecto antes da execução da operação", sendo que o agente representa uma entidade que pretende executar uma operação sobre um objecto. Estas operações resultam na dissertação nos componentes Identificação e Autenticação e Controlo Lógico de Acessos.

Nesta dimensão consideramos como *drive* principal a Identificação e Autenticação a qual valida o agente garantido consequentemente uma das principais operações de controlo de acessos lógico. A identificação pode ser baseada em algo que o utilizador conheça (ex. *password*), em algo que possui (ex. *smart cards*) ou no que é (ex. *biometria*).

DIMENSÃO	COMPONENTES	**Prováveis Indicadores** (nível de exposição)	Ex. Ameaças x Métodos de Ataque
LÓGICA[30]	1.Identificação e Autenticação	Validação pelo sistema operativo	Acesso indevido a dados, informação, serviços e / ou aplicações.
	2.Controlo Lógico de Acessos	Matriz de controlo de acesso à informação	Simular a identidade.
	3.Sistemas de Armazenamento	Sistemas de gestão documental e workflow	Manter a disponibilidade, evitando: - Falhas técnicas (ex. HW) e sistemas de suporte. - Deterioração dos meios de armazenagem e/ou falha nos equipamentos ou serviços.
		Bases de dados	
		File Server	
		Mail Server	
		Web Server	
		Aplication Server	
		Suporte de informação e formato padrão	
		Garantir dispositivos de leitura dos dados	
		Sistemas de redundância	
		Informação e dados cifrados	
	4. Gestão de logs	Clientes, servidores, activos e tecnologias de segurança.	Destruição dos logs evitando a análise forense após o ataque.
		Retenção e cópia em tempo real	
		Análise	Ausência de sincronização nos relógios dos hosts, activos, etc.
		SNTP	
	5. Outros	…	

Tabela 7 – Dimensão Lógica da Segurança da Informação

[30] Referido em SEGNAC 4 (1990), ISO/IEC 13335-4 (2000), Oliveira (2001), Carneiro (2002) e Tittel et al (*2003*).

Para realizar a análise forense computacional é necessário utilizar os *Logs* dos diversos componentes tecnológicos da rede, fundamentalmente os *logs* do sistema, que representam um papel importante na análise do sistema de ficheiros, pois permitem reconstruir o que aconteceu no sistema operativo, podendo estes ser configurados para registar entre outras actividades, as do utilizador, dos processos, dos serviços e consequentemente registar actividades não usuais que podem caracterizar uma possível infracção. Neste componente devemos garantir que a retenção e cópia dos *logs* é realizada em tempo real e simultaneamente garantir a sincronização dos relógios dos computadores.

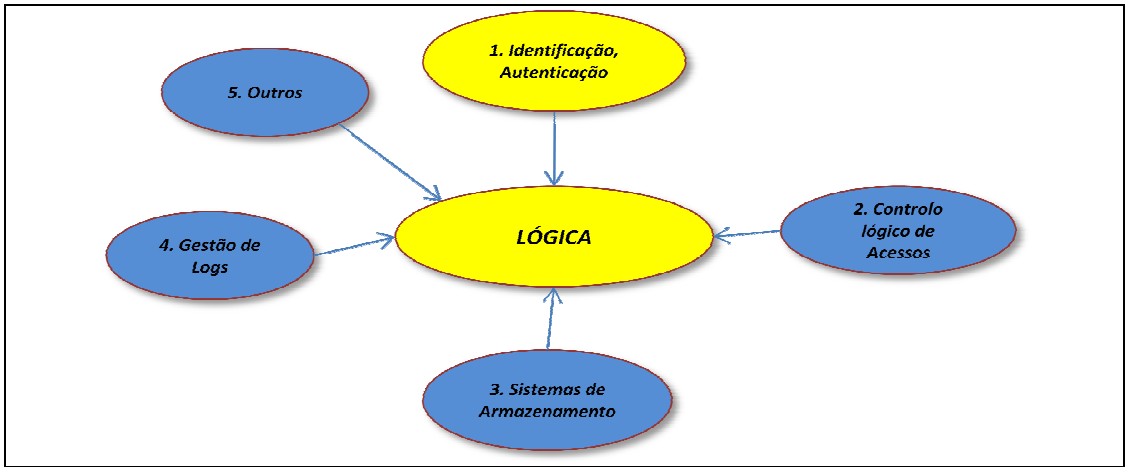


Figura 21 – Dimensão Lógica

Como conclusão deste capítulo e após a identificação e análise das dimensões, componentes e indicadores prováveis da Framework de Segurança, apresentamos uma visão macro para a segurança dos SI na Figura 22, da qual podemos concluir que a segurança dos SI tem que ser vista como um processo, que permita integrar todas as suas dimensões, derivado das diversas interdependências entre componente e indicadores.

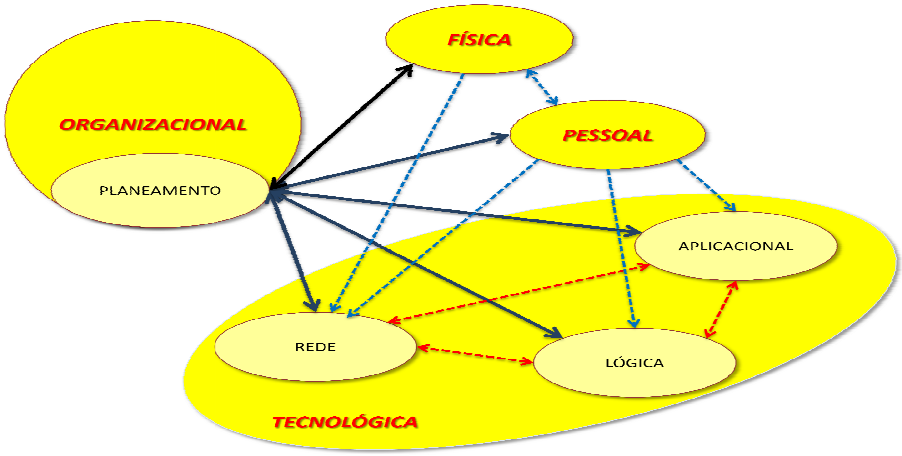


Figura 22 – Dimensões da Segurança da Informação

4. FRAMEWORK DE SEGURANÇA DE UM SI

Neste capítulo é apresentada a *Framework* de Segurança final com os componentes referidos e um possível processo para a sua aplicação sistemática que permitirá reduzir os riscos de segurança da informação nos SI organizacionais.

4.1 DIAGRAMA DE CLASSES

O motivo fundamental que nos levou a adoptar a *UML* na dissertação foi recorrer a uma linguagem que fosse capaz de facilitar a comunicação com as organizações auditadas, permitindo descrever de modo rigoroso as fases de análise, desenho, implementação e gestão da Framework de Segurança. É uma linguagem que utiliza uma notação padrão para especificar, construir, visualizar e documentar SI orientados por objectos (Nunes e O´Neill, 2001).

A Framework de Segurança encontra-se representada pelo Diagrama de Classes da UML na Figura 23, com a ideia principal de permitir-nos identificar os aspectos mais importantes que fazem parte do SI em estudo e consequentemente visualizar o SI como um todo, através das suas classes e relações.

Usamos o diagrama de classes para descrever a estrutura de informação que é utilizada no sistema, procurando descrever o seu estado (atributos) e comportamento (métodos). Representa uma abstracção sobre um conjunto de objectos, que partilham a mesma estrutura e comportamento, pois na prática um objecto é um caso particular de uma classe, também referido por instância de classe. As classes descrevem objectos com atributos e operações comuns que servem dois propósitos: permitem compreender o mundo real naquilo que é relevante para o SI que se pretende desenvolver e fornecem uma base prática para a sua implementação (Nunes e O´Neill, 2001).

Um objecto (ex. dimensão, componente ou indicador) tem um conjunto de métodos (operações) que os processos externos ao objecto podem activar e que caracterizam o seu comportamento. A semântica desses objectos define o conjunto de serviços que o objecto oferece. Os parâmetros e os resultados do método formam a interface do objecto. O código interno do objecto não é visível nem interessa aos elementos que estão fora do objecto.

O diagrama de classes apresentado na dissertação pretende fornecer uma perspectiva estática que suporta os requisitos de segurança da informação do SI em análise. A Framework através dos componentes e indicadores apresentados para as dimensões da segurança, implicitamente lista os controlos técnicos ou não técnicos [31] existentes ou planeados no SI organizacional para reduzir ou eliminar a probabilidade de uma ou mais vulnerabilidades serem exploradas por uma ameaça.

[31] Podemos estabelecer a distinção entre os tipos de controlo segundo as indicações do SP 800-30 (2001, p.20).

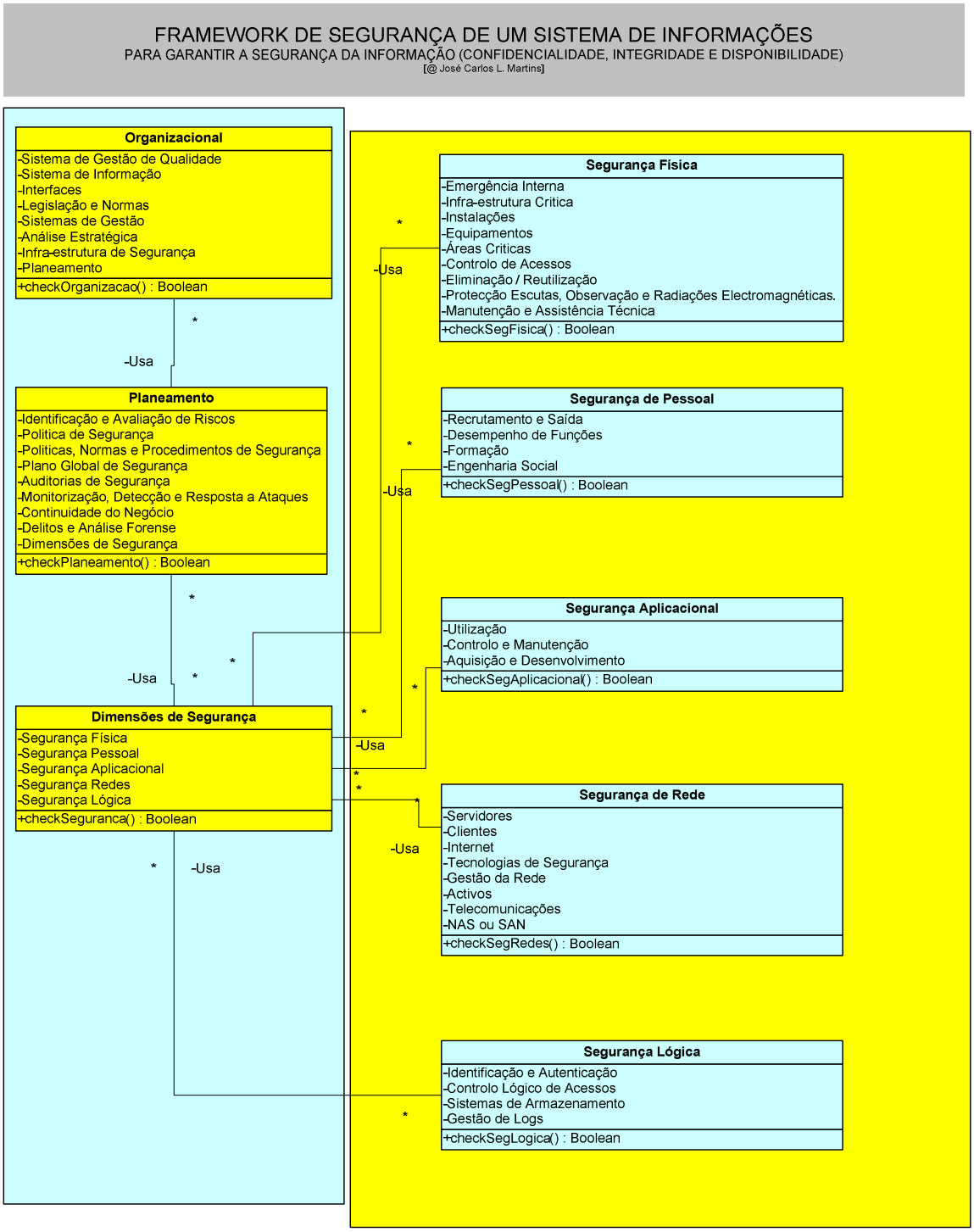


Figura 23 – Framework de Segurança da Informação

4.2 INQUÉRITO E AUDITORIA

A análise dos dados obtidos do inquérito – A conflitualidade da Informação – (Anexo B), permitiu-nos validar a existência e a importância da rede suportada em TI como base de funcionamento da organização e obtivemos a percepção dos decisores militares para alguns dos aspectos levantados nas dimensões, componentes e indicadores da *Framework* de segurança.

A análise estatística dos dados permitiu-nos confirmar que os elementos da amostra consideram a perda de segurança como uma das ameaças à utilização da informação no âmbito operacional da organização e que a segurança é reduzida face às ameaças aos sistemas, podendo deste modo reforçar a sua percepção para a necessidade da existência de uma *Framework* de Segurança.

As violações de segurança de informação afectaram fundamentalmente a disponibilidade dos recursos, não sendo referidas preocupações assinaláveis com a integridade e confidencialidade da informação.

Apesar da percepção para a necessidade de segurança da informação, na Dimensão Organizacional / Planeamento esta é quase nula. Constatamos que uma percentagem elevada da amostra, confirma a não existência de um plano global de segurança da informação, reflexo da inexistência de identificação e avaliação de riscos e de uma Política de Segurança.

Verificamos que a necessidade de formação e o desempenho de funções de acordo com o perfil de competências do colaborador saem reforçados, face à percepção dos decisores para a má preparação técnica dos utilizadores, o que possibilita toda a panóplia de ataques de Engenharia Social, tal como apresentado na Dimensão Pessoal e implicitamente levanta problemas na Dimensão Aplicacional face ao desconhecimento técnico na utilização de *software*, podendo pôr em risco a segurança da informação.

Reforçaram também a percepção para a Dimensão Física através da necessidade de mecanismos para o controlo de acessos.

Consideram os vírus como o principal e mais perigoso método de ataque, o que valida a necessidade da existência de um antivírus e reforçam a utilização de *firewalls* nas suas redes para garantir a Segurança dos SI na Dimensão Rede.

Têm a percepção para a necessidade do uso de *passwords* para o controlo de acessos, bem como realização dos *backups* à informação, confirmando consequentemente a Dimensão Lógica da segurança da informação.

O estudo exploratório realizado e apresentado, permite-nos face à operacionalização de alguns indicadores concluir que existe a percepção dos decisores para a necessidade de existirem as dimensões de segurança apresentadas na Framework de Segurança.

Em conclusão, o estudo realizado permite-nos apresentar um possível modelo conceptual para a Segurança dos SI organizacionais (Figura 24). Após a identificação e análise das ameaças e referenciados os seus possíveis métodos de ataque nos diversos componentes e indicadores das dimensões de segurança, podemos executar a sua defesa face às possíveis acções resultantes das operações de informação (Figura 25). A metodologia de aplicação foi validada pela auditoria de segurança ao CDD (Anexo D).

Figura 24 – Modelo Conceptual para a Segurança dos SI Organizacionais

Desenvolvemos na nossa perspectiva um possível modelo conceptual de defesa para fazer face a acções de Guerra de Informação / Competitive Intelligence sob os SI, tendo como referência o modelo apresentado na Figura 25.

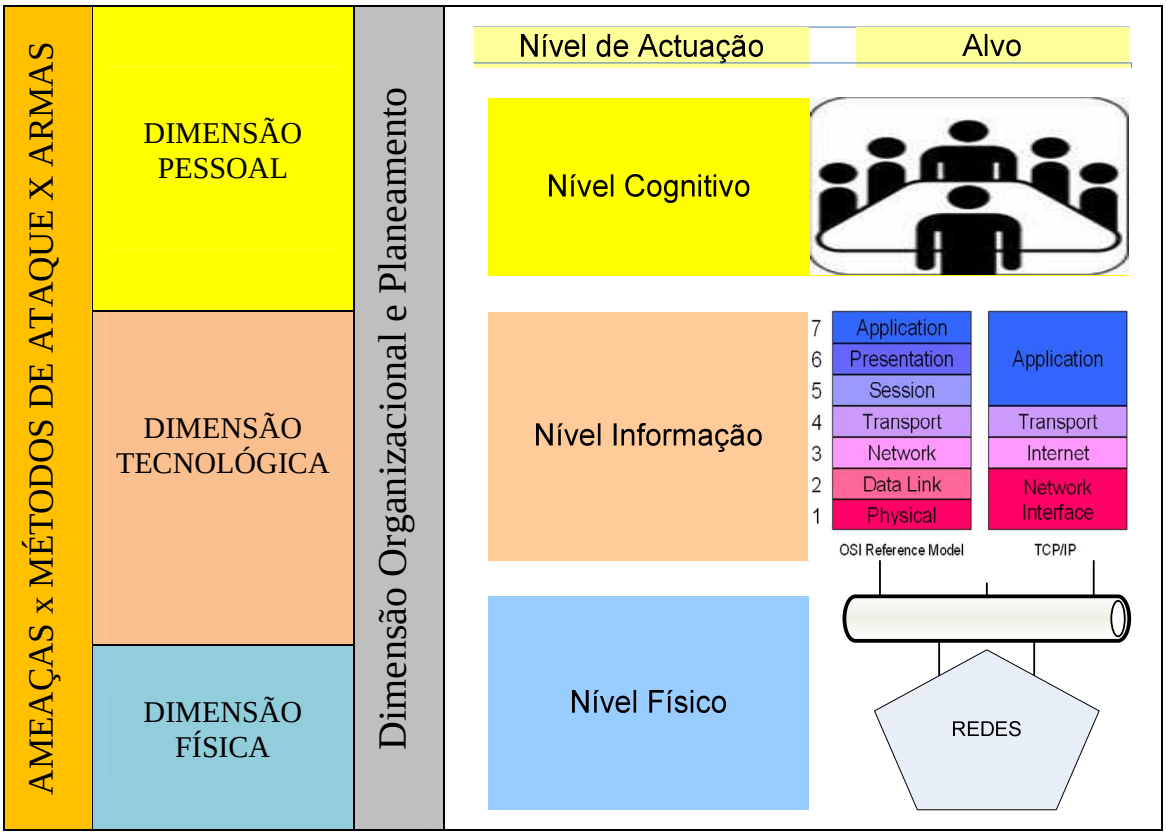


Figura 25 – Modelo Operacional de Defesa das OI

Neste modelo conceptual apresentamos as dimensões de segurança que garantem as propriedades da informação de um SI organizacional, face às possíveis acções de Guerra de Informação anteriormente apresentadas. Salientamos que a ligação entre dimensões é efectuada pelo planeamento centralizado dos controlos implementados, após a análise dos processos organizacionais.

O estudo exploratório (Anexo B) em associação com a auditoria realizada (Anexo D) permitiu-nos validar as dimensões e os componentes apresentados na *Framework* de Segurança, sendo estes facilmente percepcionados pelos decisores das organizações militares pela sua cultura de segurança, embora a dimensão Planeamento e a Pessoal seja bastante reduzida em termos de evidências obtidas na auditoria realizada.

5. CONCLUSÕES

A *Framework* de Segurança apresentada para um SI, tem como objectivo principal a segurança da informação face à Guerra de Informação / Competitive Intelligence. Esta permite integrar e interligar as dimensões indicadas, garantindo consequentemente que os indicadores dos componentes apresentados estão implementados.

A ameaça de uma Guerra de Informação Estratégica, elimina por completo a distinção entre os sistemas militares e civis (Nunes, 1999), face ao que apresentamos na dissertação, uma metodologia de identificação e análise de ameaças que representa-se o Nível Estratégico, de Gestão e Operacional.

Desta forma podemos de um modo realista perspectivar as suas intenções face às capacidades, garantindo a implementação dos controlos necessários e suficientes para a defesa dos SI organizacionais, de acordo com o binómio custo / eficácia.

Obtivemos uma *Framework* de Segurança flexível e modelar para os SI de uma organização militar, tendo a sua metodologia de implementação sido validada na auditoria à Divisão de Administração e Comunicações e Segurança do CDD (Anexo D).

Garantimos deste modo, que esta poderá servir de base para uma possível ferramenta de auditoria à segurança dos SI organizacionais militares e constituir uma metodologia útil para planear a sua política de segurança organizacional.

As vantagens que pensamos alcançar com a *Framework* apresentada e a sua metodologia de aplicação em relação a outras analisadas (ex. OCTAVE e ISO 27001) para garantir a Gestão da Segurança da Informação nos SI, são as seguintes:

- A possibilidade de integração de diversas metodologias de gestão e segurança em uso nas organizações militares (ex. a análise SWOT, a metodologia ITIL, o Plano de Emergência Interna, etc.), evitando a repetição de análises e obtendo uma visão mais de acordo com a percepção do decisor para o negócio e de fácil operacionalização.

- Permite-nos uma visão mais abrangente da segurança devido à interligação das suas diversas dimensões apresentadas, como podemos verificar através da *Framework* obtida.

- A metodologia de identificação e análise de ameaças é global, devido à integração de possíveis acções militares e à orientação conceptual apresentada na dissertação, na qual consideramos que os métodos de ataque não são mais que acções desenvolvidas por determinadas ameaças (ex. a nível estratégico, os Estados), utilizando armas (física, sintaxe ou semântica) de modo a explorar determinadas vulnerabilidades e consequentemente causando um impacto na organização.

- Facilita a identificação e avaliação do risco de segurança dos SI organizacionais, em virtude de na fase inicial não estar tão focada na avaliação do risco individual de cada activo, mas garantindo numa fase posterior a análise mais refinada para cada um dos processos e activos críticos da organização face à sua missão.

  Pela analogia com as operações defensivas militares**,** numa primeira fase a preocupação não são os sistemas de armas particulares, mas a operação defensiva no global, após o que se analisa cada sistema de armas *de per si* na contribuição para a operação defensiva geral.

- Existência de uma dimensão de planeamento integrando todas as actividades de gestão e controlo das diversas dimensões da segurança, evitando duplicações de controlos (recursos vs custos) e a necessidade de complexas coordenações.

- A utilização da linguagem UML através do seu diagrama de classes permite uma maior flexibilidade na análise, planeamento, implementação e gestão da *Framework* de Segurança aplicada à organização. Facilitando a futura integração ou alteração da composição dos indicadores existentes ou resultantes de novos métodos de ataque.

- Integramos facilmente na nossa *Framework* algumas das boas práticas de outras metodologias sem necessidade de alterar o modelo conceptual das dimensões e componentes. Validamos com a análise da metodologia OCTAVE, a qual só tem preocupações com a infra-estrutura tecnológica em termos de vulnerabilidades. Esta não considera a dimensão física e a pessoal e a sua operacionalização inicial seria eventualmente demasiado morosa (na nossa perspectiva). No entanto apresenta aspectos fundamentais a considerar futuramente na metodologia de aplicação da nossa *Framework* e dos quais salientamos:

  - A utilização de processos em cada uma das iterações da metodologia de aplicação da *Framework* de segurança. Na primeira iteração, é de considerar a Segurança dos SI organizacionais no global. Numa segunda e terceira iteração (análise dos processos e activos em cada processo), devemos considerar a utilização de *workshops* para facilitar a identificação e análise de activos críticos (suas vulnerabilidades e controlos de segurança aplicados).

  - Considerar os seus critérios de impacto (alto, médio e baixo) e a probabilidade de uma ameaça explorar uma vulnerabilidade igual a um para todas as situações, face à dificuldade do seu cálculo e à inexistência de dados objectivos (histórico de incidentes) em termos de organizações militares semelhantes e ou internos à própria organização.

As principais dificuldades sentidas na elaboração da dissertação foram:

- A abrangência de assuntos, a sua complexidade técnica e transversalidade a várias áreas do conhecimento e a normal limitação temporal.

- Acrescida pela dificuldade em descobrir o "*Estado da Arte*", pois na realidade estes assuntos possuem um valor acrescentado para as empresas de consultadoria na área da segurança da informação e para as organizações militares é considerado um assunto "tabu" ou são classificados.

- É ainda de considerar a necessidade de entrar em jogo com a percepção dos decisores sobre o real valor da informação para a sua organização e consequentemente a dificuldade em identificar e analisar algumas das vulnerabilidades das organizações.

- Finalmente, a utilização desta *Framework* exige uma permanente análise e actualização dos indicadores de segurança, em virtude de ser um processo contínuo, em permanente evolução, face à mudança dos processos internos da organização, à complexidade e evolução das TI e alteração dos recursos humanos.

COMO POSSÍVEIS ESTUDOS EM ABERTO consideramos a possibilidade de:

- Validar as dimensões, componentes e indicadores em Organizações Nacionais, tendo em consideração que sem indicadores mensuráveis para suportar uma metodologia de gestão da segurança da informação, não é possível garantir um nível de segurança da informação adequado e qualquer investimento em segurança pode ser sempre questionado (Santos, 2006).

- Desenvolver e implementar um possível modelo conceptual de defesa e ataque para as possíveis acções de Guerra de Informação num SI, focado na Cenarização de Ataques, com indicações da probabilidade de ocorrência e consequente cálculo do impacto na organização.

Para finalizar, consideramos que a segurança da informação é um processo de gestão e não um processo tecnológico (ISO 27001, 2005), no qual deve existir um equilíbrio entre a segurança Física, Pessoal, Tecnológica e Organizacional.

REFERÊNCIAS BIBLIOGRAFICAS

LIVROS

ALBERTS, Christopher e DOROFEE, Audrey (2001). *OCTAVE – Method Implementation Guide Version 2.0,* Carnegie Mellon, Software Engineering Institute, Estados Unidos da América.

ALBERTS et al (1999). *Network Centric Warfare: Developing and Leveraging Information Superiorit,* CCRP Publication Series, Washington, Estados Unidos da América.

BONIFACE, Pascal (2002). *Guerras do Amanhã*, Editora Inquérito.

CARNEIRO, Alberto (2002). *Introdução à Segurança dos Sistemas de Informação*, FCA – Editora de Informática, Lisboa.

CASTELLS, Manuel (2002). *A Era da Informação: Economia, Sociedade e Cultura, Volume I – A Sociedade em Rede.* Fundação Calouste Gulbenkian, Lisboa.

CASTELLS, Manuel (2004). *A Galáxia Internet*. Fundação Calouste Gulbenkian, Lisboa.

CHIAVENATO, Idalberto (1989). *Recursos Humanos*, Editora Atlas S.A, Lisboa.

GHIGLIONE, Rodolphe e MATALON, Benjamin (2001). *O Inquérito*, Editora Celta, 4ª Edição, Lisboa.

KUROSE, James e ROSS, Keith (2008). *Computer Networking*, Addison Wesley, 4th Edition, Estados Unidos da América.

LAUDON, Kenneth C. e LAUDON, Jane P. (2006). *Management Information Systems*, Prentice Halll, 9ª ed, Estados Unidos da América.

MACFARLANE, Ivor e RUDD, Colin (2003). *Gestão de Serviços de TI,* The IT Service Management Forum.

MARCELLA, Albert J. e GREENFIELD, Robert S. (2002). *Cyber Forensics – A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes,* Auerbach Publications.

MARQUES, José e GUEDES, Paulo (1998). *Tecnologias de Sistemas distribuídos.* FCA – Editora de Informática, Lisboa.

MITNICK, Kevin D. e SIMON, William L. (2003). *A Arte de Enganar*, Pearson Education, São Paulo.

MOREAU, Frank (2003). *Compreender e Gerir os Riscos*, Bertrand Editora, Lisboa.

MORGADO, Maria José e VEGAR, José (2003). *O Inimigo sem rosto – Fraude e Corrupção em Portugal*, Dom Quixote, Lisboa.

NORTHCUTT, Stephen (2002). *Segurança de Redes*, SANS GIAC, Editora Campos.

NUNES, Mauro e O´NEILL, Henrique (2001). *Fundamental de UML*. FCA – Editora de Informática, Lisboa.

OLIVEIRA, Wilson (2001). *Segurança da Informação*, Centro Atlântico, Lisboa.

PFLEEGER, C. P. and PFLEEGER, S. L (2007*). Security in Computing*, Prentice Hall Professional Techinical Reference, 4th ed.

QUIVY, Raymond e CAMPENHOUDT, Luc Van (2005), *Manual de Investigação em Ciências Sociais*, Gradiva. 4ª Edição, Lisboa.

SERRANO, António e FIALHO, Cândido (2003), *Gestão do Conhecimento – O Novo Paradigma das Organizações*, FCA – Editora de Informática, Lisboa.

SERRANO, António e JARDIM, Nuno (2007). *Disaster Recovery-Um Paradigma na Gestão da Continuidade*, FCA – Editora de Informática, Lisboa.

SHELLY et al (2005). *Discovering Computers – A Gateway to information*, Shelly Cashman Series.

SILVA et al (2003). *Segurança dos Sistemas de Informação*, Centro Atlântico, Lisboa.

STEVEN et al (2003). *Modelos de Gestão*, Financial Times, Prentice Hall.

TABORDA, João e FERREIRA, Miguel (2002). *Competitive Intelligence – Conceitos, Práticas e Benefícios*, Editora Pergaminho, 1ª Edição, Lisboa.

TANENBAUM, Andrew (1997). *Redes de Computadores*, Editora Campus, 3ª Edição.

TITTEL et al (2003). *Certified Information Systems Security Professional (Study Guide)*, SYBEX.

TOFFLER, Alvin (1984). *A Terceira Vaga*, Livros do Brasil, Lisboa.

TURBAN et al (2003). *Administração de Tecnologia de Informação*, Editora Campus.

VARAJÃO (1998). *A Arquitectura da Gestão de Sistemas de Informação*, FCA – Editora de Informática, Lisboa.

WADLOW, Thomas (2001). *Segurança de Redes*, Editora Campus. 1ª Edição.

WALTZ, Edward (1998). *Information Warfare: Principles and Operations*, Artech House.

TRABALHOS PUBLICADOS, ARTIGOS DE JORNAIS E REVISTAS

ALEXANDRE, Carlos (2005). *Da Competitive Intelligence à Guerra de Informação – Um Estudo sobre o Papel da Engenharia Social na Segurança de Sistemas de Informação,* Pós – Graduação em Guerra de Informação / Competitive Intelligence, Academia Militar, Lisboa.

AMARAL, L. (1994). *PRAXIS – Um Referencial para o Planeamento de Sistemas de Informação,* Tese de Doutoramento, Universidade do Minho.

BALSINHAS, Paulo (2003). *Os Riscos do Ciberespaço - Análise e Gestão dos Riscos nas Infra-Estruturas Criticas de Informação,* Pós – Graduação em Guerra de Informação / Competitive Intelligence, Academia Militar, Lisboa.

CUNHA, Paulo (2001). *Técnicas para a Análise do Negócio*, Universidade de Coimbra.

ELOFF, M. M. e SOLMS, S. H. von (2000). *Information Security Management: A Hierarchical Framework for Various Approaches,* Computers & Security, 19, p. 243-256.

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,* Computers & Security, 17, p. 303-307.

HILDRETH, Steven (2001). *Cyberwarfare, Report for Congress U.S. Congressional Research Service,* The Library of Congress, Estados Unidos da América.

HILTON, Ronald W. (1981). *The Determinants of Information Value: Synthesizing Some General Results*, Management Science, Vol. 27, No. 1, p. 57-64.

HOWARD, R.A. (1996). *Information Value Theory*, Systems Science and Cybernetics, IEEE Transactions on Volume 2, Issue 1, p. 22 – 26.

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 Nº 9, p. 135-158.

NUNES, Paulo Viegas (1999). *"Impacto das Novas Tecnologias no Meio Militar: A Guerra de Informação"*, in Vários, *Revista Militar*, p. 1721-1745.

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.

NUNES, Paulo (2008), *Apontamentos de Guerra de Informação e Competitive Intelligence*, Pós – Graduação em Guerra de Informação / Competitive Intelligence, Academia Militar, Lisboa.

RICHARDSON, Robert (2007). *The 12th Annual Computer Crime and Security Survey*, Computer Security Institute, Estados Unidos da América.

ROCHA, Álvaro (1997). *O Essencial dos Sistemas de Informação*, Universidade Fernando Pessoa.

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, Publicação da Associação Portuguesa para a Qualidade*, pp 11-1, Ano XXXV, Nº1, ISSN 0870-6743, Lisboa.

SANTOS, Henrique (2008). *Apontamentos de Segurança Digital*, Pós – Graduação em Guerra de Informação / Competitive Intelligence, Academia Militar, Lisboa.

SARMENTO, Manuela (2005). *Seminário de Modelos de Gestão e Competitividade*, Pós – Graduação em Guerra de Informação / Competitive Intelligence, Academia Militar, Lisboa.

SOLMS, Rossouw Von e POSTHUMUS, Shaun (2004). *A framework for the governance of information security*, Computers & Security, 23, p. 638- 646.

NORMATIVOS

BS 7799–3 (2006). *Information Security- Managements Systems*, Part 3: Guidelines for Information Security Risk Management.

COBIT 4.0 (2005). *Control Objectives – Management Guidelines – Maturity Models*, IT Governance Institute, Estados Unidos da América.

EN ISO 9000 (2000) *Sistemas de gestão da qualidade, fundamentos e vocabulário*. Norma Portuguesa.

EN ISO 9001 (2000). *Sistemas de gestão da qualidade, requisitos*. Norma Portuguesa.

BS ISO / IEC 17799 (2005). *Information technology – Security techniques – Code of practice for information security management. British Standards.*

ISO /IEC: 27001(2005). *Information technology – Security techniques – Information Security Management Systems - Requirements.*

ISO / IEC TR 13335-1 (2004). *Information technology- Security techniques-Management of information and communications technology security. Part 1: Concepts and models for information and communication technology security management.*

ISO / IEC TR 13335-3(1998). *Information technology- Guidelines for the management of IT Security. Part 3: techniques for the management of IT security.*

ISO / IEC TR 13335-4(2000). *Information technology- Guidelines for the management of IT Security. Part 4: Selection of safeguards.*

ISO / IEC TR 13335-5(2001). *Information technology-Guidelines for the management of IT Security. Part 5: Management guidance on network security.*

NIST SP 800-26 (2001). *Computer Security – Security Self-Assessment Guide for Information Tecnology Systems.*

NIST SP 800-30 (2001). *Risk Management - Guide for Information Technology Systems.*

NIST SP 800-42 (2001). *Computer Security – Guideline on Network Security Testing*.

LEGISLAÇÃO NACIONAL

SEGNAC 1 (1988). *Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas*. D.R I Série, 279 (03-12-1988), 4772-4800.

SEGNAC 2 (1989). *Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial, Tecnológica e de Investigação*. D.R I Série, 245 (14-10-1989), 4672-4700.

SEGNAC 3 (1994). *Instruções para a Segurança Nacional-Segurança das Telecomunicações,* D.R I Série B, 68 (22-03-1994), 1423-1427.

SEGNAC 4 (1990). *Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática*. D.R I Série, 49 (28-02-1990), 806 (2) - 806 (17).

DOUTRINA MILITAR

AC/35-D / 2000 – REV3 (Julho 2007). *Directive Personnel Security*, NATO Security Committee.

AC/35-D / 2001 – REV1 (Dezembro 2006). *Directive Physical Security*, NATO Security Committee.

AC/35-D / 2002 – REV3 (Dezembro 2006). *Directive on the Security of Information*, NATO Security Committee.

AC/35-D / 2003 - REV3 (Dezembro 2006). *Directive on Industrial Security*, NATO Security Committee.

AC/35-D / 2004 – REV1 (Outubro 2006). *Primary Directive on INFOSEC*, NATO Security Committee.

AC/35-D / 2005 – REV1 (Outubro 2006). *INFOSEC Management Directive for Communication and Information Systems (CIS*, NATO Security Committee.

CM 49 (2002). *Security Within The North Atlantic Treaty Organisation*, NATO Security Committee.

DCSI / EME (2007). *Elemento de Guerra de Informação – Estrutura e Implicações*, MDN / Exército / EME, Lisboa.

FM 100-06 (1996). *Information Operations*, Headquarters, Department of the Army, Washington, Estados Unidos da América.

FM 3-13 (2003). *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, Headquarters, Department of the Army, Washington, Estados Unidos da América.

JP 3 – 13 (2006). *Joint Doctrine for Information Operation*, Estados Unidos da América.

JP 3 – 13.1 (1996). *Joint Doctrine for Command and Control Warfare*, Estados Unidos da América.

RAD 280-1 (2003). *Segurança da Informação Armazenada, Processada ou Transmitida nos Sistemas de Informação e Comunicação do Exército*. Estado Maior do Exército / Exército Português /Ministério da Defesa Nacional.

SAS – 050 (2006). *Exploring New Command and Control Concepts and Capabilities*, Final Report, Prepared for NATO.

ANEXOS

ANEXO A – FORMULÁRIO DE ANÁLISE DE ACTORES

Pós Graduação em Guerra de Informação e Competitive Intelligence - 2007/08

Exercício "The Day After in… Cyberspace"

Formulário de Análise de Actores

Identificação do Actor

Nome: _____

Origem: _____

Dt Criação: _____

Pontos Fortes:

Pontos Fracos:

Centro de Gravidade:

Motivações:

Estados Finais Pretendidos:

Presença Geográfica:

Relações relevantes do Actor com 3ºs

Actor: _____ Relação:

Actor: _____ Relação:

Actor: _____ Relação:

Actor: _____ Relação:

Actor: _____ Relação:

Actor: _____ Relação:

Representação dos Interesses / Recursos dos Actores em Jogo

Avaliação da sua Importância:

- ○ 100% Civilizacional: sobrevivência da raça humana
- ○ 90%
- ○ 80%
- ○ 70% Social: ambição, destino, cultura, educação
- ○ 60%
- ○ 50%
- ○ 40%
- ○ 30% Colectiva: demands, projectos, valores, conceitos
- ○ 20%
- ○ 10%
- ○ 0% Individual: necessidades, desejos, regras, conhecimento

Avaliação do Conhecimento para Agir:

- ○ 100% Completamente informado para agir preemptivamente
- ○ 90% Marioritariamente informado para agir preemptivamente
- ◉ 80% Completamente informado para agir decisivamente
- ○ 70% Marioritariamente informado para agir preemptivamente
- ○ 60% Marioritariamente informado para agir eficientemente
- ○ 50% Razoavelmente informado para agir eficientemente
- ○ 40% Pouco informado para agir eficientemente
- ○ 30% Razoavelmente informado para agir de forma positiva
- ○ 20% Pouco informado para agir de forma positiva
- ○ 10% Pouco informado para qualquer tipo de acção
- ○ 0% Sem qualquer informação para agir

Avaliação da sua Capacidade para Agir:

- ○ 100% Potência Global (EUA)
- ○ 90% Potência Continental (UE)
- ○ 80% Potência Regional (China, Rússia)
- ○ 70% Média Potência/Nação (Espanha, Itália)
- ○ 60% Pequena Potência/Nação (Suiça, Portugal)
- ○ 50% Nação Muito Pequena, Negócio Global
- ○ 40% Grande Negócio, Rede Criminosa
- ○ 30% Médio Negócio, Grupo terrorista,Grande ONG
- ◉ 20% Pequeno Negócio, Família Rica, ONG
- ○ 10% Família Normal, Homem armado
- ○ 0% Homem Isolado, sem nada

Avaliação da sua Vontade para Agir:

- ○ 100% Totalmente preparado para morrer na acção
- ○ 90% Razoavelmente preparado para morrer na acção
- ○ 80% Totalmente empenhado para agir decisivamente
- ○ 70% Marioritariamente empenhado para agir decisivamente
- ◉ 60% Totalmente empenhado em agir com eficácia
- ○ 50% Marioritariamente empenhado em agir com eficácia
- ○ 40% Pouco empenhado em agir com eficácia
- ○ 30% Marioritariamente pronto para agir de forma positiva
- ○ 20% Pouca prontidão para agir de forma positiva
- ○ 10% Razoavelmente paralisado pelos seus sentimentos
- ○ 0% Completamente paralisado pelos seus sentimentos

Avaliação da Legitimidade para Agir:

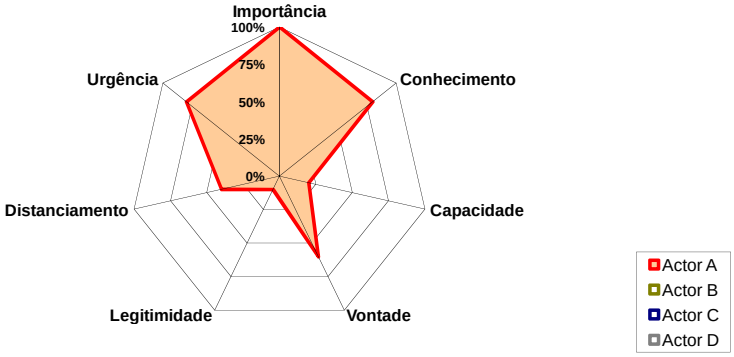
- ○ 100% Completamente autorizado a agir de qualquer forma
- ○ 90% Razoavelmente autorizado a agir de qualquer forma
- ○ 80% Completamente autorizado a agir decisivamente
- ○ 70% Maioritariamente autorizado a agir decisivamente
- ○ 60% Ligeiramente restringido a agir eficientemente
- ○ 50% Razoavelmente restringido a agir eficientemente
- ○ 40% Maioritariamente restringido a agir eficientemente
- ○ 30% Razoavelmente restringido a agir de forma positiva
- ○ 20% Maioritariamente restringido a agir de forma positiva
- ◉ 10% Maioritariamente paralisado pelo seu sentimento de culpa
- ○ 0% Completamente paralisado pelo seu sentimento de culpa

Avaliação do seu Distanciamento:

- ○ 100% Interesse não preservado / nada realizado
- ○ 90%
- ○ 80% Interesse pouco preservado / realizado
- ○ 70%
- ○ 60%
- ○ 50% Interesse parcialmente preservado / realizado
- ◉ 40%
- ○ 30% Interesse maioritariamente preservado / realizado
- ○ 20%
- ○ 10%
- ○ 0% Interesse completamente preservado / realizado

Avaliação da sua Urgência:

- ○ 100% Segundos
- ○ 90% Minutos
- ◉ 80% Horas
- ○ 70% Dias
- ○ 60% Semanas
- ○ 50% Meses
- ○ 40% Anos
- ○ 30% Décadas
- ○ 20% Gerações
- ○ 10% Séculos
- ○ 0% Nenhuma



ANEXO B – PERCEPÇÃO DA CONFLITUALIDADE DA INFORMAÇÃO

APÊNDICE B.1 – METODOLOGIA E RESULTADOS DA ANÁLISE

Pretendemos obter a percepção dos decisores militares para a conflitualidade da informação, com base num inquérito como instrumento metodológico (Anexo B – Apêndice 03), representando apenas um estudo exploratório e não permitindo generalizar.

A elaboração do inquérito não foi realizada de base para validar a Framework de Segurança, no entanto podemos verificar que algumas das questões permitem a operacionalização de alguns dos indicadores da *Framework* da segurança apresentada.

As questões derivadas que foram levantadas para obter dos responsáveis dos sistemas de informação de organismos militares nacionais, as suas percepções sobre a conflitualidade da informação, numa rede informática são as seguintes:

- Será que a base de funcionamento da organização é a rede? (Questão 1)

- Serão os SI importantes nos níveis do processo de decisão e actividades? (Questão 2)

- Existem ameaças e vulnerabilidades à segurança da informação? (Questão 3)

- Existiram violações na segurança da informação? (Questão 4)

- Existem preocupações com a segurança da informação? (Questão 5)

- Existe plano global de segurança e actores de segurança? (Questão 6)

- Há utilização operacional da informação? (Questão 7)

METODOLOGIA

Com base no **universo** de oficiais do quadro permanente das Forças Armadas, foi realizado um inquérito a elementos do Curso de Estado-Maior no âmbito do seu trabalho individual de longa duração subordinado ao tema "A conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação" e aplicado no contexto da organização militar.

O **processo de amostragem,** não teve por base uma amostra aleatória e consequentemente não manteve a proporcionalidade em relação ao universo, mas apesar disso permitiu-nos obter a sua percepção para alguns dos indicadores.

A **amostra** foi constituída por setenta e dois (72) Oficiais do quadro permanente dos três ramos das Forças Armadas Portuguesas (Exército, Força Aérea, Marinha), com o Posto de Coronel ou Major.

O **instrumento** metodológico e **procedimento de aplicação** foi a entrevista directa e pessoal através da aplicação de um inquérito, em que as questões colocadas se distinguem quanto à forma em questões fechadas e abertas. As questões abertas foram agrupadas num pequeno número de categorias pela análise de conteúdos, após o que tratamos como questões fechadas. Nas questões procuramos obter apenas a percepção, efectuando uma análise estatística descritiva. O questionário reflecte as boas práticas de elaboração e aplicação (Ghiglione & Matalon, 2001), de onde salientamos:

- Foi usado o mesmo inquérito para todas as pessoas inquiridas sem explicações suplementares e não foi efectuada qualquer modificação no enunciado das questões e na sua ordenação.

- Não existiram pontos imprecisos ou a necessitar de explicações para além daquelas que estão explicitamente previstas e o vocabulário é simples.

- As questões procuram não sugerir qualquer resposta particular, não exprimir qualquer expectativa e não excluir nada do que possa passar pela cabeça da pessoa a quem se vai colocar.

- Permite saber, se à pessoa que vamos inquirir, se aplica o questionário.

- As questões fechadas e abertas encontram – se explicitamente agrupada pelo tema e nas questões fechadas, a sua instrução revestiu-se de formas muito diferentes, sendo as mais usuais: o indicar a resposta mais adequada ou indicar várias respostas, sendo livre o número de respostas possíveis.

Identificamos e enquadramos a amostra (Área IV – Identificação da amostra), definimos o perfil de utilização operacional das tecnologias de informação e comunicação nas organizações (Área I), após o que procuramos obter a percepção em termos de ameaças e vulnerabilidades na segurança da informação, numa rede informática (LAN) de uma organização militar ligada à Internet, verificando se existem e quais as suas preocupações com a segurança física, de rede e lógica (Área II – Impacto Organizacional da Utilização Conflitual da Informação).

Neste inquérito procurou – se simultaneamente avaliar, quais os reflexos operacionais da utilização competitiva e conflitual da informação no contexto da actual sociedade de informação, segundo as suas envolventes civis e militares (Área III – Análise SWOT - Relativa à utilização Operacional da Informação no Contexto Organizacional), sendo para efeitos da dissertação um aspecto pouco explorado.

Procuramos com este inquérito, efectuar apenas uma análise de dados através de estatística descritiva, de modo a obter uma percepção da amostra em estudo, procurando validar algumas das dimensões, componentes e indicadores apresentados.

Nas percepções da amostra para a necessidade de segurança física, de rede e lógica, consideramos o risco de colocar o " […] indivíduo perante a nossa própria concepção do fenómeno a estudar, obrigando a aceitar a nossa interpretação pessoal e sabendo que os resultados a obter, serão apenas o que à partida inserimos." (Ghiglione & Matalon, 2001, p. 04), no entanto reforçamos a ideia de que este estudo exploratório apenas pretende obter a percepção para a problemática da segurança dos SI nas organizações militares.

As dimensões de segurança aplicacional e pessoal não foram abordadas directamente neste inquérito, mas através da análise *SWOT*, obtivemos alguns dados que reflectem a sua percepção para estas dimensões.

Com a Tabela 08 apresentamos as variáveis (indicadores) que permitem orientar a resposta da amostra para cada uma das questões levantadas.

Tabela 08 – Relação Variáveis e Questões

Questões	Caracterização das variáveis / indicadores de percepção (inquérito)
01	VAR04; VAR05; VAR06
02	VAR01; VAR02; VAR03
03	VAR08; VAR11
04	VAR07; VAR09
05	VAR10; VAR12; VAR13; VAR16; VAR17; VAR18; VAR19
06	VAR14; VAR15
07	VAR20; VAR21; VAR22; VAR23

A **descrição das variáveis** é a indicada sucintamente na Tabela 09 e que nos permitiu obter a percepção para as questões levantadas e simultaneamente validar alguns dos indicadores da *Framework* de segurança:

Tabela 09 – Descrição de Variáveis

VAR01	Utilização dos sistemas de informação (SI) e das tecnologias de informação e comunicação (TIC) na organização.
VAR02	Nível de organização em que SI e TIC assumem maior importância no processo de tomada de decisão.
VAR03	Actividades da organização em que as TIC assumem maior importância no funcionamento.
VAR04	Rede como base de funcionamento na organização.
VAR05	Actividade da organização dependente da utilização de uma ligação à Internet.
VAR06	Importância do funcionamento em rede na organização para a competitividade / eficiência.
VAR07	Violações de segurança da informação, em que afectaram a organização.
VAR08	Origem dos problemas verificados na área de segurança da informação na organização.
VAR09	Data da última violação de segurança da informação, na organização.
VAR10	Soluções para a protecção de Redes e dos SI, na organização.
VAR12	Responsável pela realização de *backups* de informação, na organização.

VAR13	Periodicidade da realização de *backups* de informação, na organização.
VAR14	Responsável pela administração e segurança das redes e dos SI, na organização.
VAR15	Plano de segurança da informação na organização.
VAR16	Importância com a segurança informática e de telecomunicações nos últimos 5 anos (1999 até 2004), na organização.
VAR17	Evolução no próximo ano nos investimentos em sistemas de segurança informática e de telecomunicações na organização.
VAR18	Nível de segurança da organização em questões de segurança informática e de telecomunicações.
VAR19	Formas de ataque mais perigosas para a segurança da informação na organização.
VAR20	Vantagens da utilização da informação no âmbito operacional da organização.
VAR21	Desvantagens da utilização da informação no âmbito operacional da organização.
VAR22	Oportunidades da utilização da informação no âmbito operacional da organização.
VAR23	Ameaças, da utilização da informação no âmbito operacional da organização.

RESULTADOS DA ANÁLISE

Consideramos importante salientar, que o objectivo fundamental deste inquérito, é a obtenção da percepção para as ameaças e vulnerabilidades à segurança da informação, numa organização militar.

Após obtermos os inquéritos preenchidos, efectuamos a codificação e introdução dos dados (Anexo B / Apêndice 2 - Codificação dos Dados), efectuando análises estatísticas do tipo descritivo e obtendo apenas as frequências de cada categoria para as variáveis em análise. **Da análise dos dados, obtivemos as seguintes percepções:**

A rede é a base de funcionamento da organização, considerada como muito elevada e elevada a importância desta tipologia, apesar da actividade da organização não depender da ligação à Internet (Questão 01).

Consideram como importante e muito importante a utilização dos SI, assumindo maior importância na tomada de decisões ao nível da gestão intermédia e no funcionamento das actividades primárias (Questão 02).

As violações de segurança de informação afectaram fundamentalmente a disponibilidade dos recursos, considerando os ataques de vírus como a sua principal e mais perigosa ameaça externa (forma de ataque) e a nível interno a má preparação técnica dos utilizadores da rede (Questões 03 e 04).

Como principal solução para a protecção de redes e de SI admitem a existência de um software antivírus, no entanto consideram a necessidade de mecanismos para a protecção ao nível das diversas dimensões da segurança: física através do controlo de acessos, segurança de redes pela utilização de *firewalls* e lógica pelo uso de *passwords* (Questão 05).

Existe um responsável pela administração e segurança das redes e dos SI, sendo da sua responsabilidade a realização dos *backups* à informação, com periodicidade fundamentalmente diária, apesar da percepção para a responsabilização dos utilizadores na actividade da cópia de segurança de informação (Questão 06).

Numa percentagem elevada (54,17%), não existe um plano de segurança da informação. Apesar da importância com a segurança informática e de telecomunicações nos últimos 5 anos ter aumentado, bem como um aumento previsto nos investimentos em sistemas de segurança informática e de telecomunicações, consideram vulneráveis as organizações em segurança informática e de telecomunicações (Questão 06).

Das vantagens da utilização da informação no âmbito operacional da organização, salienta-se o número de elementos que não respondem (20 elementos) e foram referidos fundamentalmente os seguintes aspectos:

- A importância no apoio à decisão e ao comando e controlo.
- A partilha de dados, informação e conhecimento.
- Permitir uma gestão mais eficaz e eficiente no cumprimento da missão.
- A redução de recursos humanos, materiais e custos.
- Rapidez de acesso e difusão de dados / informação.

Das desvantagens da utilização da informação no âmbito operacional da organização, salienta-se o número de elementos que não respondem (24 elementos) e foram referidos fundamentalmente os seguintes aspectos:

- Segurança reduzida face às ameaças aos sistemas.
- Fracos conhecimentos de TI na generalidade dos militares.
- Falta de informação fiável e em excesso.
- Fraca integração entre os vários sistemas de informação e instabilidade dos sistemas.
- Inflexibilidade e dependência dos sistemas / máquinas pelo utilizador.

Nas oportunidades da utilização da informação no âmbito operacional da organização, salienta-se o número de elementos que não respondem (31 elementos) e foram referidos fundamentalmente os seguintes aspectos:

- Divulgação e abertura ao mundo civil pela organização.
- Acesso mais fácil a novas tecnologias, à informação e ao conhecimento.
- Aumento da eficiência e da vantagem competitiva em relação a outras organizações.

Nas ameaças da utilização da informação no âmbito operacional da organização, salienta-se o número de elementos que não respondem (38 elementos) e foram referidos fundamentalmente os seguintes aspectos:

- A perda de segurança.
- Falta de objectividade e excesso de informação.
- A constante readaptação a dinâmicas impostas do exterior, com custos.
- Incapacidade de se adaptar a estas novas realidades.
- A concepção dos sistemas aplicacionais.

APÊNDICE B.2 – ANÁLISE DESCRITIVA DAS VARIÁVEIS

Variável em análise (VAR01): Utilização dos sistemas de informação (SI) e das tecnologias de informação e comunicação (TIC) na organização. Variável ordinal, da qual podemos verificar, que a percepção é: para considerar como importante e muito importante a utilização dos sistemas de informação (SI) e das tecnologias de informação e comunicação (TIC) na sua organização.

Tabela 10 – Distribuição da variável 01

Categorias	Frequências	%
Muito Importante	47	65,28
Importante	25	34,72
Pouco Importante	0	0
Negligenciável	0	0
Não Responde	0	0
Total	72	100

Variável em análise (VAR02): Nível de organização em que SI e TIC assumem maior importância no processo de tomada de decisão. Variável nominal, da qual podemos verificar que a percepção é: de considerar ao nível da gestão intermédia uma maior importância na tomada de decisões, sendo equivalente nos níveis de gestão de topo e operacional.

Tabela 11 – Distribuição da variável 02

Categorias	Frequências	%
Gestão de Topo	11	15,28
Gestão Intermédia	45	62,50
Gestão Operacional	8	11,11
Não Responde	8	11,11
Total	72	100

Variável em análise (VAR03): Actividades da organização em que as TIC assumem maior importância no funcionamento. Variável nominal, da qual podemos verificar que a percepção é: de considerar uma maior importância das TIC no funcionamento das actividades primárias.

Tabela 12 – Distribuição da variável 03

Categorias	Frequências	%
Administração	16	22,22
Actividades Primárias	32	44,44
Actividades de Apoio	17	23,61
Não Responde	7	9,72
Total	72	100

Variável em análise (VAR04): Rede como base de funcionamento na organização. Variável nominal da qual podemos verificar que a percepção é: de considerar que a rede é a base de funcionamento.

Tabela 13 – Distribuição da variável 04

Categorias	Frequências	%
Sim	60	83,33
Não	12	16,67
Não Responde	0	0
Total	72	100

Variável em análise (VAR05): Actividade da organização dependente da utilização de uma ligação à Internet. Variável nominal da qual podemos verificar que a percepção é: que a organização não está dependente da utilização de uma ligação à Internet.

Tabela 14 – Distribuição da variável 05.

Categorias	Frequências	Percentagem
Sim	18	25
Não	54	75
Não Responde	0	0
Total	72	100

Variável em análise (VAR06): Importância do funcionamento em rede na organização para a competitividade / eficiência. Variável ordinal da qual podemos verificar que a percepção é: de considerar como muito elevada e elevada a importância do funcionamento em rede.

Tabela 15 – Distribuição da variável 06.

Categorias	Frequências	%
Muito Elevada	35	48,61
Elevada	29	40,28
Moderada	7	9,72
Reduzida	0	0
Não Responde	1	1,39
Total	72	100

Variável em análise (VAR07): Violações de segurança da informação, em que afectaram a organização (Pode responder a várias opções). Variável nominal da qual podemos verificar que a percepção é: de considerar que as violações de segurança de informação, afectaram fundamentalmente a disponibilidade dos recursos quando necessários, no entanto o peso é semelhante pelos vários tipos de violação.

Tabela 16 – Distribuição da variável 07.

Categorias	Frequências	%
Confidencialidade	14	19,44 +→ 54,16
Integridade	10	13,89 +→ 48,61
Disponibilidade	21	29,17 +→ 63,89
Todos os Anteriores	25	34,72
Não Responde	9	12,50

Variável em análise (VAR08): Origem dos problemas verificados na área de segurança da informação na organização (Pode responder a várias opções). Variável nominal da qual podemos verificar que a percepção é: de considerar o ataque de vírus, como o problema que mais frequentemente se verifica na área da segurança da informação.

Tabela 17 – Distribuição da variável 08.

Categorias	Frequências	%
Ataque de Vírus	55	76,39
Roubo de Informação	0	0
Ataques por inundação	8	11,11
Ataques de intrusão interna	5	6,94
Ataques de intrusão externa	5	6,94
Não Responde	10	13,89

Variável em análise (VAR09): Data da última violação de segurança da informação, na organização. Variável ordinal da qual podemos verificar que a percepção é: de considerar com mais frequência, como data da última violação de segurança da informação, os últimos 6 meses, no entanto um grande número de elementos não responde.

Tabela 18 – Distribuição da variável 09.

Categorias	Frequências	%
Último Mês	11	15,28
Últimos 6 Meses	22	30,56
Últimos 12 Meses	8	11,11
Últimos 24 Meses	11	15,28
Não Responde	20	27,78
TOTAL	72	100

Variável em análise (VAR10): Soluções para a protecção de Redes e dos SI, na organização (Pode responder a várias opções). Variável nominal da qual podemos verificar que a percepção é: de considerar como principal solução para a protecção de redes e dos sistemas de informação, a existência de um software Anti – Vírus, podendo observar que existe segurança dos três tipos (física, redes e lógica) e que todos respondem.

Tabela 19 – Distribuição da variável 10.

Categorias	Frequências	%
Software Anti – Vírus	58	80,56
Firewall de Rede	26	36,11
Password Individual e Controlo de Acessos à Rede	54	75,00
Sistemas de Controlo Físico de Acessos	24	33,33
Não Responde	0	0

Variável em análise (VAR11): Principais fontes de quebras de segurança da informação na organização (Pode responder a várias opções). Variável nominal da qual podemos verificar que a percepção é: de considerar a má preparação técnica dos utilizadores da rede como a principal fonte de quebra de segurança da informação. Reflecte a gravidade de ataques de engenharia social.

Tabela 20 – Distribuição da variável 11.

Categorias	Frequências	%
Má Gestão da Rede Informática	20	27,78
Má preparação técnica dos utilizadores da rede	46	63,89
Acção de Agentes de Origem Interna	8	11,11
Acção de Agentes de Origem Externa	13	18,06
Não Responde	5	6,94

Variável em análise (VAR12): Responsável pela realização de *backups* (segurança lógica) de informação, na organização (Pode responder a várias opções). Variável nominal da qual podemos verificar que a percepção é: de considerar como responsável pela realização de *backups* da informação o gestor da rede.

Tabela 21 – Distribuição da variável 12.

Categorias	Frequências	Percentagem
Dos utilizadores	29	40,28
Do gestor de rede	44	61,11
Não se realizam backups	4	5,56
Não Responde	3	4,17

Variável em análise (VAR13): Periodicidade da realização de *backups* de informação, na organização (Pode responder a várias opções). Variável ordinal da qual podemos verificar que a percepção é: de considerar como diária a periodicidade de realização de *backups* da informação.

Tabela 22 – Distribuição da variável 13.

Categorias	Frequências	%
Diária	22	30,56
Semanal	20	27,78
Mensal	21	29,17
Anual ou Superior	8	11,11
Não Responde	2	2,78

Variável em análise (VAR14): Responsável pela administração e segurança das redes e dos SI, na organização. Variável nominal da qual podemos verificar que a percepção é: que existe uma entidade / órgão responsável pela administração e segurança das redes e dos SI, na organização.

Tabela 23 – Distribuição da variável 14.

Categorias	Frequências	%
Sim	61	84,72
Não	10	13,89
Não Responde	1	1,39
Total	72	100

Variável em análise (VAR15): Plano de segurança da informação, na organização. Variável nominal da qual podemos verificar que a percepção é: que não existe plano de segurança da informação.

Tabela 24 – Distribuição da variável 15.

Categorias	Frequências	%
Sim	26	36,11
Não	39	54,17
Não Responde	7	9,72
Total	72	100

Variável em análise (VAR16): Importância com a segurança informática e de telecomunicações nos últimos 5 anos (1999 até 2004), na organização. Variável ordinal da qual podemos verificar que a percepção é: que existe e cada vez é mais importante.

Tabela 25 – Distribuição da variável 16.

Categorias	Frequências	%
Muito mais importância	13	18,06
Mais importância	39	54,17
A mesma importância	18	25,00
Menos importância	2	2,78
Não Responde	0	0
Total	72	100

Variável em análise (VAR17): Evolução no próximo ano nos investimentos em sistemas de segurança informática e de telecomunicações na organização. Variável ordinal da qual podemos verificar que a percepção é: que no próximo ano os investimentos em sistemas de segurança informática e de telecomunicações na organização, aumentarão.

Tabela 26 – Distribuição da variável 17.

Categorias	Frequências	%
Aumentarão muito	3	4,17
Aumentarão	37	51,39
Manter – se – ão	28	38,89
Diminuirão	3	4,17
Não Responde	1	1,39
Total	72	100

Variável em análise (VAR18): Nível de segurança da organização em questões de segurança informática e de telecomunicações. Variável ordinal da qual podemos verificar que a percepção é: que a segurança da organização em questões de segurança informática e de telecomunicações é vulnerável

Tabela 27 – Distribuição da variável 18.

Categorias	Frequências	%
Vulnerável	36	50,00
Pouco Vulnerável	15	20,83
Muito Segura	15	20,83
Quase inexpugnável	2	2,78
Não Responde	4	5,56
Total	72	100

Variável em análise (VAR19): Formas de ataque mais perigosas para a segurança da informação na organização. Variável ordinal da qual podemos verificar que a percepção é: que o ataque de vírus é a forma mais perigosa para a organização. Elevado número de elementos que não respondem.

Tabela 28 – Distribuição da variável 19 (considerando todos os inquéritos)

Categorias	Valor da Escala
Ataque de Vírus	3,042
Roubo de Informação nas Redes de Comunicação	2,333
Ataques por Inundação	1,833
Ataques de intrusão interna	1,889
Ataques de intrusão externa	2,222
Total	72

Escala: 1 = Menos Perigoso e 5 = mais Perigoso

Tabela 29 – Distribuição da variável 19 (sem considerar as respostas nulas)

Categorias	Valor da Escala
Ataque de Vírus	3,982
Roubo de Informação nas Redes de Comunicação	3,055
Ataques por Inundação	2,4
Ataques de intrusão interna	2,473
Ataques de intrusão externa	2,909
Total	55

Escala: 1 = Menos Perigoso e 5 = mais Perigoso

Variável em análise (VAR20): Vantagens da utilização da informação no âmbito operacional da organização.

Tabela 30 – Distribuição da variável 20.

Categorias	Número de Respostas
1. Não Responde.	20
2. Rapidez no acesso e difusão de dados / informação.	34
3. Redução de recursos / custos (efectivos / materiais).	13
4. Gestão mais eficiente e eficaz (cumprimento missão)	08
5. Partilha de dados / informação / conhecimentos.	16
6. Apoio à decisão e ao comando e controlo.	14
7. Valorização pessoal.	02
8. Actualização automática de dados / informação e não redundância.	03
9. Segurança.	01
10. Racionalização da informação no seu manuseamento.	01

Variável em análise (VAR21): Desvantagens da utilização da informação no âmbito operacional da organização.

Tabela 31 – Distribuição da variável 21.

Categorias	Número de Respostas
1. Não Responde.	24
2. Inflexibilidade e dependência dos sistemas / máquinas.	07
3. Segurança reduzida face a ameaças aos sistemas (confidencialidade / integridade / disponibilidade).	20
4. Fracos conhecimentos de TI, da generalidade dos militares.	07
5. Falta de informação fiável e em excesso.	13
6. Fraca integração entre os vários sistemas de informação (logística, pessoal, etc.) e estabilidade dos sistemas.	04
7. Utilização para fins particulares e "agarra" pessoas ao PC.	02
8. Excesso de burocracia e informalidade.	03
9. Circulação interna de documentos que afectem o moral do pessoal.	01
10. Nenhuma.	02

Variável em análise (VAR22): Oportunidades da utilização da informação no âmbito operacional da organização.

Tabela 32 – Distribuição da variável 22.

Categorias	Número de Respostas
1. Não Responde.	31
2. Divulgação da organização / imagem / actividades / concursos.	14
3. Acesso a novas tecnologias, à informação / conhecimento, mais Facilmente.	20
4. Abertura ao mundo civil, entidades envolventes e partilha de Informação.	07
5. Vantagem comparativa a qualquer outra organização.	02
6. Aumento da eficiência.	05
7. Integração / Interoperabilidade.	05
8. Admissão de recursos humanos e aproveitamento de técnicos qualificados.	02
9. Não tenho conhecimento.	01

Variável em análise (VAR23): Ameaças, da utilização da informação no âmbito operacional da organização.

Tabela 33 – Distribuição da variável 23.

Categorias	Número de Respostas
1. Não Responde.	38
2. Concepção de sistemas aplicacionais.	03
3. Perda de segurança.	22
4. Falta de objectividade na informação e excesso.	06
5. Incapacidade de se adaptar a estas novas realidades.	03
6. Constante readaptação a dinâmicas impostas do exterior, com custos.	04
7. Desconhecidas.	02
8. Cidadãos esclarecidos e exigentes.	01

APÊNDICE B.3 – INQUÉRITO

MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS
INSTITUTO DE ALTOS ESTUDOS MILITARES

CURSO DE ESTADO-MAIOR 2002-04

QUESTIONÁRIO

O presente questionário insere-se no âmbito da realização do Trabalho Individual de Longa Duração (TILD) do CEM 2002-04, subordinado ao tema "A Conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação" e destina-se a ser preenchido por detentores de Cargos de Direcção e de Gestão de áreas funcionais de organizações militares e civis. No contexto militar, o público-alvo deste questionário são os Oficiais do QP dos 3 Ramos das Forças Armadas, com o Posto de:

- **Coronel ou Capitão de Mar e Guerra**, que já tenham comandado/chefiado uma Unidade Orgânica Tipo (UOT) – Regimento, Base Aérea, Navio ou equivalente.

- **Tenente-Coronel/Capitão de Fragata ou Major/Capitão-Tenente**, que já tenham desempenhado funções de Estado-Maior no âmbito de uma UOT.

A finalidade deste questionário é a de permitir avaliar, quais os reflexos operacionais da utilização competitiva e conflitual da informação no contexto da actual Sociedade de Informação, segundo as suas envolventes civis e militares.

Tendo por fundamento a realidade das organizações militares e civis, conforme percepcionada pelos detentores dos seus Cargos de Gestão, este questionário procura também realizar uma análise SWOT (*Strengths, Weaknesses, Opportunities and Threats*) com base nos diferentes aspectos operacionais associados à utilização da Informação.

O Autor do Trabalho gostaria de agradecer toda a sua disponibilidade e atenção demonstrada no preenchimento deste questionário que, espera, possa vir a contribuir para um tratamento objectivo e consequente do tema abordado.

O questionário é ANÓNIMO e CONFIDENCIAL.

ÁREA I – Perfil de Utilização Operacional das Tecnologias de Informação e Comunicação (TIC) nas Organizações

Por favor, na qualidade de Gestor de Topo/ Comandante de UOT, ou de Gestor Funcional/ elemento do Estado-Maior de uma UOT, responda assinalando, apenas a opção que considera mais correcta.

1. Considera que o **grau de utilização dos Sistemas de Informação e das Tecnologias de Informação e Comunicação (TIC)** na sua organização (UOT) pode ser considerado:

Muito Importante	☐
Importante	☐
Pouco Importante	☐
Negligenciavel	☐

2. No **processo de tomada de decisão** da sua organização, os Sistemas de Informação e as TIC assumem maior importância ao nível da:

Gestão de Topo/ Comando da UOT	☐
Gestão Intermédia/ Estado-Maior da UOT	☐
Gestão Operacional/ Secções e Subunidades da UOT	☐

3. No **funcionamento** da sua organização, as TIC assumem maior importância ao nível da:

Administração/ Comando da UOT	☐
Actividades Primárias/ (Instrução, Operações/Informações, Logística, Assuntos Civis da UOT)	☐
Actividades de Apoio (Segurança, Pessoal, Finanças da UOT)	☐

4. A sua organização utiliza uma **Rede como base de funcionamento**?

   Sim ☐
   Não ☐

5. A actividade da sua organização depende da **utilização de uma ligação à Internet**?

   Sim ☐
   Não ☐

6. Considera que a **importância do funcionamento em rede**, na competitividade/eficiência da sua organização (UOT), pode ser considerada:

Muito Elevada	
Elevada	
Moderada	
Reduzida	

ÁREA II – Impacto Organizacional da Utilização Conflitual da Informação

7. As **violações de segurança da informação** ocorridas na sua organização (UOT) afectaram:

O Acesso selectivo e controlado aos Recursos (Confidencialidade)	
A Correcta Operação dos Recursos (Integridade)	
A Disponibilidade dos Recursos quando Necessários (Disponibilidade)	
Todos os aspectos anteriores	

8. Os **problemas verificados na área da segurança da informação** da sua organização (UOT) deveram-se essencialmente a:

Ataque de Vírus	
Roubo de informação nas redes de comunicação	
Ataques por inundação (ex: Negação de Serviço)	
Ataques de intrusão interna	
Ataques de intrusão externa	

9. A **data da última violação de segurança da informação** na sua organização (UOT) teve lugar no:

Último Mês	
Últimos 6 Meses	
Ùltimos 12 Meses	
Ùltimos 24 Meses	

10. Das soluções indicadas, assinale as que são utilizadas para a **protecção das redes e dos sistemas de informação** da sua organização:

Software Anti-Vírus	☐
Firewall de Rede	☐
Password Individual e Controlo de Acessos à Rede	☐
Sistemas de Controlo Físico de Acessos	☐

11. A **principal fonte de quebras de segurança**, no que se refere à informação da sua organização, pode ser considerada:

Má Gestão da Rede Informática	☐
Má Preparação Técnica dos Utilizadores da Rede	☐
Acção de Agentes de Origem Interna	☐
Acção de Agentes de Origem Externa	☐

12. A **responsabilidade da realização de backups da informação** na sua organização é:

Dos Utilizadores	☐
Do Gestor da Rede	☐
Não são realizados backups	☐

13. A **periodicidade dos backups de informação** pode ser considerada:

Diária	☐
Semanal	☐
Mensal	☐
Anual ou Superior	☐

14. Existe uma Entidade/Órgão responsável pela **administração e Segurança das Redes e dos Sistemas de Informação** na sua organização (UOT)?

Sim ☐
Não ☐

15. Existe um **Plano de Segurança da Informação** na sua organização (UOT)?

Sim ☐
Não ☐

16. Tomando como base os últimos 5 anos, qual o nível de **importância que as questões relacionadas com a segurança informática e de telecomunicações receberam no último ano** na sua organização face aos anos anteriores?

Muito mais importância	
Mais importância	
A mesma importância	
Menos importância	

17. Como prevê que **evoluam os investimentos em sistemas de segurança informática e de telecomunicações em 2004** na sua organização ?

Aumentarão muito	
Aumentarão	
Manter-se-ão	
Diminuirão	

18. Qual considera ser o **nível de segurança da sua organização** no que se refere a questões de segurança informática e de telecomunicações (vírus, intrusão, …)?

Vulnerável	
Pouco Vulnerável	
Muito segura	
Quase inexpugnável	

19. Na sua opinião, quais as **formas de ataque que considera mais perigosas** para a sua organização? (Escala: 1 = menos perigoso e 5 = mais perigoso)

Ataque de Vírus	
Roubo de informação nas redes de comunicação	
Ataques por inundação (ex: Negação de Serviço)	
Ataques de intrusão interna	
Ataques de intrusão externa	

ÁREA III – Análise SWOT Relativa à Utilização Operacional da Informação no contexto Organizacional

20. Face ao papel que a utilização da informação assume no âmbito operacional da organização (UOT) em que presta ou prestou serviço, quais considera serem as **vantagens (forças)** e **desvantagens (fraquezas)** daí decorrentes?

    a. **Vantagens (Forças)**?

    .

    b. **Desvantagens (Fraquezas)**?

    .

21. Tendo em vista essencialmente a interacção da organização (UOT) com o ambiente exterior e a utilização competitiva e conflitual da informação, quais são as principais **oportunidades** e **ameaças** que o meio envolvente (Exército, Forças Armadas, meio civil, ambiente de mercado, etc.) oferece à sua organização (UOT)?

    a. Oportunidades?

    .

    b. Ameaças?

    .

ÁREA IV – Identificação da Amostra

No caso de não ser militar, continue o preenchimento do questionário na questão Nº 26

22. No caso de ser militar, indique qual o seu Posto:

Coronel / Capitão de Mar e Guerra ☐ Tenente-Coronel /Capitão de Fragata ☐ Major / Capitão-Tenente ☐

23. O Ramo das Forças Armadas a que pertence:

Marinha ☐ Exército ☐ Força Aérea ☐

24. Indique qual o tipo de Unidade que Comandou/Chefiou ou de que fez parte do respectivo Estado-Maior (Assinale apenas a colocação em que permaneceu mais tempo com o actual posto):

Regimento/Base Aérea/Navio ☐ Escola ☐ Direcção Administrativa ☐

Centro de Informática ☐ Direcção Logística ☐ Outro tipo de Unidade ☐

25. Durante quanto tempo exerceu essas funções?

Menos de 12 Meses ☐ Entre 1 e 2 Anos ☐ Mais de 2 Anos ☐

O preenchimento do seu questionário termina aqui.

26. No âmbito da sua organização ocupa actualmente um cargo de:

Direcção ou Gestão de Topo ☐ Coordenação ou Gestão Operacional ☐

Direcção ou Gestão Intermédia ☐ Outro tipo de Cargo ☐

27. Indique qual o tipo da Organização a que pertence:

Administração Pública/Estado ☐ Grande Empresa ☐ Empresa ligada às Tecnologias de Informação ☐

Pequena/Média Empresa ☐ Multinacional ☐ Outro tipo de Organização ☐

28. Durante quanto tempo exerceu ou exerce essas funções?

Menos de 12 Meses ☐ Entre 1 e 2 Anos ☐ Mais de 2 Anos ☐

Obrigado pela disponibilidade demonstrada no preenchimento deste questionário.

Os dados fornecidos serão mantidos CONFIDENCIAIS e utilizados no âmbito do Trabalho Individual de Longa Duração (TILD), do CEM 2002-2004, subordinado ao tema:

"A Conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação".

ANEXO C – PRESTAÇÃO DE SERVIÇOS PARA A CERTIFICAÇÃO BS7799-2:2002

(OMITIDO - CLASSIFICADO)

ANEXO D – RELATÓRIO DE AUDITORIA AO CDD

(OMITIDO - CLASSIFICADO)

ANEXO E – PLANO DE EMERGÊNCIA INTERNO DE UMA ORGANIZAÇÃO

(OMITIDO - CLASSIFICADO)