Lusíada
Repositório das Universidades Lusíada

Universidades Lusíada

Casaca, Joaquim António Aurélio, 1958-
Correia, Maria Manuela Marques Faia, 1967-

Governo da segurança da informação : uma abordagem à realidade empresarial portuguesa

http://hdl.handle.net/11067/1026
https://doi.org/10.34628/g71w-kt86

Metadados

Data de Publicação 2013

Resumo A protecção dos activos de informação das organizações é conseguida através de uma estratégia e políticas de segurança que permitam, entre outros factores, gerir e avaliar os riscos da segurança, alocar correctamente os recursos e estar em conformidade com as leis, regulamentos e políticas de segurança. O governo da segurança da informação é o processo de gestão mais adequado para garantir que a informação esteja protegida de ameaças à sua confidencialidade, integridade e disponibilidade. Este ...

Palavras Chave Pequenas e médias epresas - Medidas de segurança, Processamento de dados, Segurança informática, Sistemas de informação para a gestão - Medidas de segurança

Tipo article

Revisão de Pares Não

Coleções [ULL-FCHS] LPIS, n. 08 (2013)

Esta página foi gerada automaticamente em 2024-11-14T19:22:29Z com informação proveniente do Repositório

http://repositorio.ulusiada.pt

GOVERNO DA SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM À REALIDADE EMPRESARIAL PORTUGUESA

Joaquim António Casaca
Professor Auxiliar no ISLA Campus Lisboa
joaquim.casaca@lx.isla.pt
Manuela Faia Correia
Professora Associada da Universidade Lusíada de Lisboa
mcorreia@lis.ulusiada.pt

Resumo

A protecção dos activos de informação das organizações é conseguida através de uma estratégia e políticas de segurança que permitam, entre outros factores, gerir e avaliar os riscos da segurança, alocar correctamente os recursos e estar em conformidade com as leis, regulamentos e políticas de segurança. O governo da segurança da informação é o processo de gestão mais adequado para garantir que a informação esteja protegida de ameaças à sua confidencialidade, integridade e disponibilidade.

Este artigo tem como objectivo primordial conhecer a importância que as empresas portuguesas atribuem ao facto de estarem em conformidade com as normas e regulamentos sobre a segurança da informação; qual o seu nível de conhecimento das normas e regulamentos existentes; saber se as empresas portuguesas possuem um programa de segurança da informação e qual a sua percepção sobre a estratégia adoptada na protecção dos seus activos informacionais e a forma como os recursos (humanos e técnicos) são afectos a essa estratégia. Esta investigação foi realizada com base num inquérito junto de 156 empresas.

Os resultados mostram que as empresas portuguesas estão pouco sensibilizadas para as questões relacionadas com o governo da segurança da informação e que a sua maioria não conhece as principais normas e regulamentações que suportam os programas de segurança da informação. Concluiu-se, ainda, que os principais elementos do governo da segurança da informação não estão presentes na acção global da gestão executiva dessas empresas.

Palavras-chave:

segurança da informação, governo segurança da informação, modelos segurança da informação, conformidade, normas e regulamentos.

Abstract

The protection of organizational information assets of is achieved through a strategy and security policies which in turn allow to manage and evaluate the security risks, the proper allocation of resources and the compliance with

laws, regulations and security policies. The information security governance is the most appropriate management process to ensure that the information is protected from threats to its confidentiality, integrity and availability.

This article objectives are to reveal the importance that compliance with information security rules and regulations assumes to Portuguese companies and what is their level of knowledge of existing rules and regulations and to know if Portuguese companies have an information security program and their perception of the strategy to protect their assets and how informational resources (human and technical) are allocated to this strategy. This research was based on a survey to 156 companies.

The results show that Portuguese companies are aware of some issues about the information security governance and that the majority do not know the main rules and regulations that support the information security programs. It was concluded, that the main elements of information security governance are not present in the overall action of the executive management of these companies.

Keywords

information security, information security governance, information security models, compliance, regulations and standards.

Introdução

Até muito recentemente, a preocupação com a protecção dos activos informacionais das empresas tem estado focalizada nos SI/TIC e não na própria informação, fazendo com que a segurança dos SI/TIC fosse circunscrita à segurança da informação dentro dos limites do domínio tecnológico da infra-estrutura de rede (ITGI, 2006).

A informação é um componente indispensável na condução do negócio da maioria das organizações (Knapp & Marshall, 2007). As organizações actuais já não são caracterizadas pelos seus activos físicos, mas por pessoas que criam, processam e distribuem informação (Dhillon & Backhouse, 2000). A informação é a base dos processos de negócio e o meio de obter vantagem competitiva sobre a concorrência, tornando-se, assim, um activo crítico no desempenho das organizações e, como tal, deve ser protegido adequadamente (von Solms & von Solms, 2006).

Enquanto a segurança dos SI/TIC diz respeito à segurança da tecnologia, a segurança da informação trata, por um lado, os riscos, benefícios e processos relacionados com a informação e, por outro lado, com todos os aspectos da informação (falada, escrita, impressa, electrónica ou baseada em qualquer outro meio) e do seu tratamento (criação, transporte, armazenamento e destruição), enquadrando todos os processos da informação, físicos e electrónicos, envolvendo, não só pessoas e tecnologia, como também, relações com parceiros, clientes e terceiros (ITGI, 2006).

A crescente dependência das organizações na sua informação e nos sistemas que a tratam (recolha, processamento, armazenamento e distribuição), juntamente com os riscos, benefícios e oportunidades que os recursos informacionais apresentam, fazem com que o governo da segurança da informação seja um factor cada vez mais crítico na governação global e, segundo Krehnke (2007), esteja essencialmente focado em acrescentar valor e mitigar os riscos relativos à segurança da informação. Se a informação é um recurso crítico e fundamental para o futuro das organizações, então a sua protecção deve ser uma tarefa da administração e as actividades da segurança da informação devem ser integradas e constituir-se como parte integrante do governo da organização (Pironti, 2006; Poore, 2007; von Solms & von Solms, 2006).

Apesar de muitas organizações adoptarem uma abordagem à segurança

da informação centrada na tecnologia (Caralli & Wilson, 2004), a segurança da informação passou de um problema técnico, da responsabilidade da direcção de sistemas de informação, a um problema do negócio (Caralli, 2004) e da governação, a qual é responsável por garantir que "as actividades apropriadas da segurança da informação estão sendo executadas de modo a que os riscos sejam reduzidos de forma apropriada e os investimentos da segurança da informação sejam direccionados adequadamente" (Fitzgerald, 2007, p. 16). Estas actividades requerem o envolvimento efectivo da gestão para avaliar as ameaças e definir as respostas a essas ameaças (von Solms, 2001a; National Cyber Security Summit Task Force [NCSSTF] 2004; Knapp & Marshall, 2007). Se, porventura, este envolvimento da gestão não se verifique e a responsabilidade pela segurança da informação for delegada num nível organizacional que careça de autoridade, responsabilidade e de recursos para actuar em conformidade com os objectivos, assistir-se-á a um completo falhanço da implementação de uma política eficaz da segurança da informação na organização (Allen, 2005).

Em função do exposto, é importante conhecer:

1. Qual a importância que as empresas portuguesas atribuem ao facto de estarem em conformidade com as normas e regulamentos sobre a segurança da informação e qual o seu nível de conhecimento das normas e regulamentos existentes;
2. Se as empresas portuguesas possuem um programa de segurança da informação e qual a sua percepção sobre a estratégia adoptada na protecção dos seus activos informacionais e a forma como os recursos (humanos e técnicos) são afectos a essa estratégia.

Complementarmente, pretende-se analisar se a dimensão e o tipo de empresa têm alguma relação com a existência (ou não) de incidentes de segurança, com o facto das empresas terem implementado (ou não) um programa de segurança da informação e com a obrigatoriedade (ou não) de respeitarem uma determinada norma ou regulamento sobre a segurança da informação.

Para tentar responder a estas questões, este artigo faz uma breve resenha da literatura relevante nesta matéria, abordando os aspectos sobre as características do governo da segurança da informação, os modelos mais importantes na implementação de uma política de segurança da informação e os modelos de maturidade utilizados para avaliar essas políticas. De seguida procede-se à análise dos dados recolhidos em função dos objectivos atrás enunciados e, por último, discutem-se os resultados e apresentam-se as principais conclusões.

Características do Governo da Segurança da Informação

O governo da segurança da informação pode ser definido como um subconjunto do governo da organização que "providencia orientação estratégica, assegura que os objectivos são alcançados, gere os riscos de forma apropriada, utiliza os recursos organizacionais de modo responsável e monitoriza o sucesso ou falhanço do programa de segurança da organização" (ITGI, 2006, p. 17),

garantindo-se, desta forma, a execução das seguintes funções (Moulton & Coles, 2003):

- responsabilidades e práticas da segurança;
- estratégias e objectivos para a segurança;
- gestão e avaliação dos riscos;
- gestão dos recursos da segurança;
- conformidade com a legislação, regulamentos e políticas de segurança.

Para Westby e Allen (2007), o governo da segurança da informação está alicerçado num conjunto de 14 actividades, integradas em quatro categorias distintas, como apresentado no Quadro 1.

Quadro 1: Categorias e actividades do governo da segurança da informação.

Categoria	Actividade
Estrutura	• Definir a estrutura de governo. • Atribuir papéis e responsabilidades, definindo linhas de comunicação. • Desenvolver políticas de alto nível.
Activos e Responsabilidades	• Inventariar activos de informação. • Desenvolver e actualizar descrições dos sistemas. • Definir e actualizar a propriedade e custódia dos activos. • Designar responsabilidades de segurança e segregação de deveres.
Conformidade	• Determinar e actualizar requisitos de conformidade. • Mapear activos com a tabela de autoridade. • Mapear e analisar os fluxos de informação.
Avaliação e Estratégia	• Realizar avaliação de ameaças, vulnerabilidades e risco. • Determinar critérios operacionais. • Desenvolver e actualizar plano de gestão de risco. • Desenvolver e actualizar estratégia de segurança da organização.

Fonte: Adaptado de Westby e Allen (2007).

Uma execução adequada destas funções permite obter um conjunto de benefícios do governo da segurança da informação, que para o ITGI (2006) se podem resumir a:

- redução da incerteza das operações do negócio através da redução dos riscos relacionados com a segurança da informação para níveis aceitáveis pela organização;
- optimização da utilização dos recursos escassos de segurança;
- eficiente e efectiva gestão do risco, melhoria de processos e resposta rápida a incidentes de segurança;
- garantia da implementação de uma eficaz política de segurança da informação e conformidade da mesma com leis e regulamentos;
- garantia de que as decisões críticas não são tomadas com base em informação defeituosa.

Por outro lado, o governo da segurança da informação deve estar alinhado com o governo dos SI/TIC, para que, segundo Doherty e Fulford (2006), se possa assegurar que as acções resultantes do planeamento estratégico dos SI/TIC não sejam comprometidas por problemas com a sua segurança, o que implica a revisão ou modificação da política de segurança da informação sempre que seja definida uma nova estratégia dos SI/TIC ou se verifique uma alteração da estratégia já implementada.

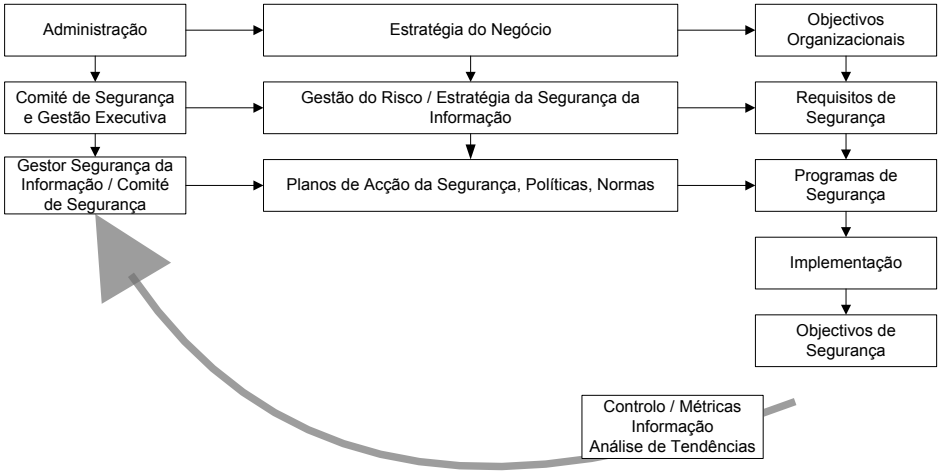
Modelos de Governo da Segurança da Informação

Para a maioria das organizações, a implementação de uma efectiva política de governo da segurança da informação é uma actividade fundamental, dado que, de uma forma geral, as acções sobre segurança da informação são fragmentadas e de natureza táctica, i.e., sem direcção da gestão (ITGI, 2008). Existem diversos modelos para desenvolver um governo da segurança da informação, devendo cada organização adoptar aquele que melhor se adapte às suas necessidades e objectivos.

A Figura 1 apresenta o modelo de governo da segurança da informação proposto pelo ITGI (2006), o qual assenta nas seguintes características:

- uma metodologia para a gestão do risco da segurança da informação;
- uma estratégia de segurança alinhada com os objectivos do negócio e dos SI/TIC;
- uma estrutura organizacional adequada;
- políticas de segurança que tratem de todas as questões da estratégia, controlo e regulação;
- um conjunto de normas de segurança para cada política para assegurar que os procedimentos e orientações estão em conformidade com a política;
- institucionalização de processos de monitorização para assegurar conformidade e providenciar informação sobre a mitigação dos riscos;
- um processo que assegure avaliação contínua e actualização das políticas de segurança, normas, procedimentos e riscos.

Figura 1: Modelo para o governo da segurança da informação.



Fonte: ITGI (2006, p. 19).

O NCSSTF (2004) propõe um modelo de governo da segurança da informação composto pelas seguintes áreas de governo:

- autoridade e funções da administração, gestão executiva e gestão intermédia;
- responsabilidades de todos os empregados e utilizadores;
- unidade organizacional para o programa de segurança;
- unidade organizacional de prestação de informação;
- avaliação do programa de segurança da informação.

Como forma de implementar este modelo de governo, o NCSSTF recomenda a utilização do modelo IDEAL (*Initiating, Diagnosing, Establishing, Acting, Learning), desenvolvido pelo SEI/CMU, o qual apresenta uma abordagem para a melhoria contínua, definindo os passos necessários para que seja possível obter um programa de melhoria bem sucedido. O Quadro* 2 apresenta as cinco fases e as 15 actividades que compõem este modelo.

Quadro 2: Fases e actividades do modelo IDEAL.

Fase	Designação	Actividades
Iniciar	Planear os alicerces para um esforço de melhoria de sucesso.	• Estímulos para a mudança. • Definir o contexto. • Constituir patrocínio. • Mapear infra-estruturas.
Diagnosticar	Determinar onde se está e para onde se pretende ir.	• Características actuais e estados desejados. • Desenvolver recomendações.
Determinar	Desenvolver um plano de trabalho detalhado.	• Definir prioridades. • Desenvolver abordagem. • Planear acções.
Actuar	Realizar o trabalho de acordo com o planeado nas fases anteriores.	• Criar solução. • Testar solução. • Refinar solução. • Implementar solução.
Aprender	Rever o que foi realizado e determinar como implementar melhorias de forma mais eficiente no futuro.	• Analisar e validar. • Propor acções futuras.

Fonte: Gremba e Myers (1997).

Partindo do conceito de governo da segurança da informação anteriormente descrito, von Solms e von Solms (2006) apresentam um modelo, que denominam de "Ciclo Dirigir-Controlar", transversal a todos os níveis da organização e parte integrante e fundamental do governo da segurança da informação, conforme representado na Figura 2.

Este modelo baseia-se no princípio de que compete à gestão dirigir e controlar a organização, i.e., fornecer orientação estratégica através de políticas, normas e procedimentos para o funcionamento da organização e assegurar que a organização está em conformidade, não só com as leis nacionais ou sectoriais, mas também com as políticas, normas e procedimentos definidos internamente.

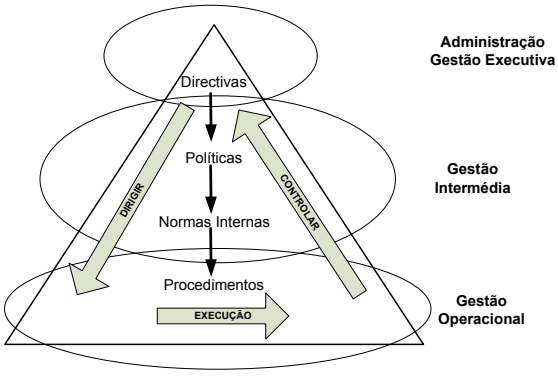


Figura 2: Modelo "Ciclo Dirigir--Controlar".

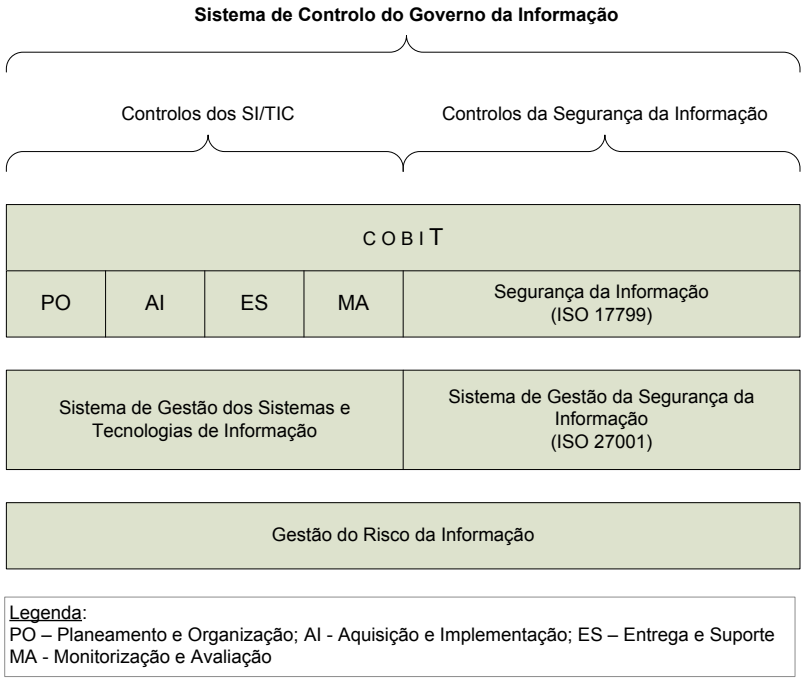
Fonte: von Solms e von Solms (2006, p. 409).

Nos modelos atrás referidos, todos, sem excepção, apresentam uma única estrutura organizacional responsável pela implementação e controlo da política estratégica da segurança da informação não manifestando, contudo, qualquer necessidade de segregação de funções ao nível da realização das tarefas e do respectivo controlo.

Todavia, S. H. von Solms (2005) advoga que o governo da segurança da informação deve ser decomposto em duas funções distintas: gestão operacional da segurança da informação e a gestão da conformidade da segurança da informação, cada uma delas suportada numa estrutura organizacional distinta, na medida em que uma é responsável pela execução das actividades técnicas e não técnicas relacionadas com a implementação dos controlos, políticas e procedimentos de segurança e, a outra, é responsável pela monitorização e avaliação da conformidade dos controlos implementados.

Para Poole (2006) um modelo efectivo da segurança da informação é aquele que combina o melhor do CobiT e da ISO 177991, pois permite alcançar os objectivos da organização em matéria de governação empresarial, concentrando-se no controlo e na responsabilização, como apresentado na Figura 3.

Figura 3: Modelo de controlo do governo da segurança da informação.



Fonte: Poole (2006, p. 3).

[1] Esta norma veio dar origem à ISO/IEC 27001 (designação que foi utilizada no inquérito às empresas).

Por seu lado, B. von Solms (2005) defende que estas duas normas são complementares e que se as empresas as usarem em conjunto podem obter sinergias, apontando, no entanto, vantagens e desvantagens na utilização de cada uma delas, sintetizadas no Quadro 3.

Quadro 3: Vantagens e desvantagens do CobiT e ISO 17799.

Norma	Vantagem	Desvantagem
CobiT	Segurança da informação é integrada num modelo vasto de governo dos SI/TIC, composto por 33 processos.	Nem sempre é muito detalhado em termos de "como" executar determinadas tarefas.
ISO 17799	Muito detalhado e fornece mais orientação em "como" realizar as tarefas	Norma isolada e não integrada num modelo mais vasto de governo dos SI/ TIC.

Fonte: Adaptado de B. von Solms (2005).

O Quadro 4 apresenta os modelos e as normas mais importantes que poderão servir de base para um efectivo governo da segurança da informação.

Quadro 4: Modelos e normas para implementação do governo da segurança da informação.

Modelo / Norma	Aplicação	Âmbito	Importância para o Governo da Segurança da Informação
ISO 17799	Internacional	Gestão da segurança da informação.	Gestão das práticas de segurança da informação.
CobiT	Internacional	Controlo e segurança de TIC.	Objectivos de controlo para a segurança de TIC e processos de controlo.
ITIL	Internacional	Gestão de serviços de TIC.	Serviços de TIC e práticas de gestão de operações que contribuem para a segurança.
ISF – The Standard	Internacional	Segurança da informação.	Práticas de segurança da informação.
NIST SP 800-14	Sobretudo EUA	Segurança de sistemas de informação.	Práticas de segurança da informação concentradas nos sistemas.
NIST SP 800-53	Sobretudo EUA	Segurança de sistemas de informação.	Abordagem para seleccionar e especificar controlos de segurança.
FIPS 200	Sobretudo EUA	Segurança de sistemas de informação.	Define os controlos mínimos para garantir a segurança dos sistemas de informação.

Modelo / Norma	Aplicação	Âmbito	Importância para o Governo da Segurança da Informação
HIPAA	EUA	Segurança de dados.	Práticas de segurança da informação concentradas na informação e nos dados.
CMMI e outros modelos de maturidade	Internacional	Processos de melhoria.	Estrutura para a melhoria dos processos e maturidade.

Fonte: Caralli (2004, p 40).

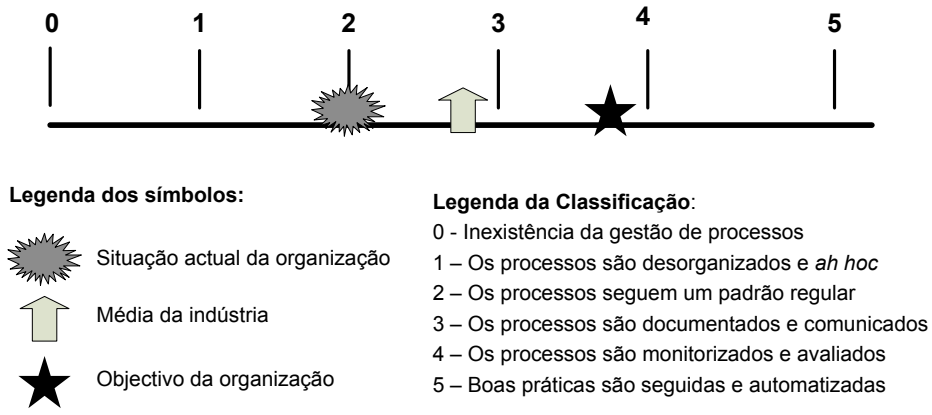
De todas as considerações que foram efectuadas sobre as características e propriedades do governo da segurança da informação, resulta claro que, para se conseguir alcançar um desempenho eficaz neste domínio, é necessário a existência de uma cultura de segurança que observe os seguintes requisitos (Westby & Allen, 2007):

- a segurança da informação é gerida em todas as vertentes da organização;
- os gestores são responsáveis pela segurança da informação perante todas as partes com interesses na organização;
- a segurança da informação é entendida como um requisito do negócio;
- a segurança da informação é determinada em função da análise de risco;
- os papéis, responsabilidades e segregação de funções estão claramente definidos no âmbito da segurança da informação;
- a segurança da informação assenta em políticas e procedimentos suportados por pessoas, processos e tecnologia;
- os recursos estão devidamente atribuídos às funções e actividades da segurança da informação;
- o pessoal tem formação adequada e conhecimento acerca da problemática da segurança da informação;
- os requisitos de segurança são definidos de acordo com o ciclo de vida dos activos de informação;
- a segurança da informação é planeada, gerida e avaliada como parte integrante da estratégia da organização;
- a segurança da informação é avaliada e auditada periodicamente.

Avaliação do Governo da Segurança da Informação

O ITGI (2006, 2008) propõe que a avaliação da governação da segurança da informação seja efectuada através do modelo de maturidade adoptado pelo CobiT 4.1 (ITGI, 2007), constante da Figura 4, o qual permite, não só posicionar a organização em termos de desenvolvimento do seu programa de governação, mas, simultaneamente, efectuar uma comparação com a média da indústria da qual a organização faz parte.

Figura 4: Modelo de maturidade do governo da segurança da informação.



Fonte: ITGI (2006, p. 36).

As várias fases do modelo de maturidade constantes do Quadro 5, estão associadas a três factores fundamentais: a gestão do risco; as responsabilidades pela segurança da informação; a continuidade do serviço das tecnologias de informação e comunicação (TIC).

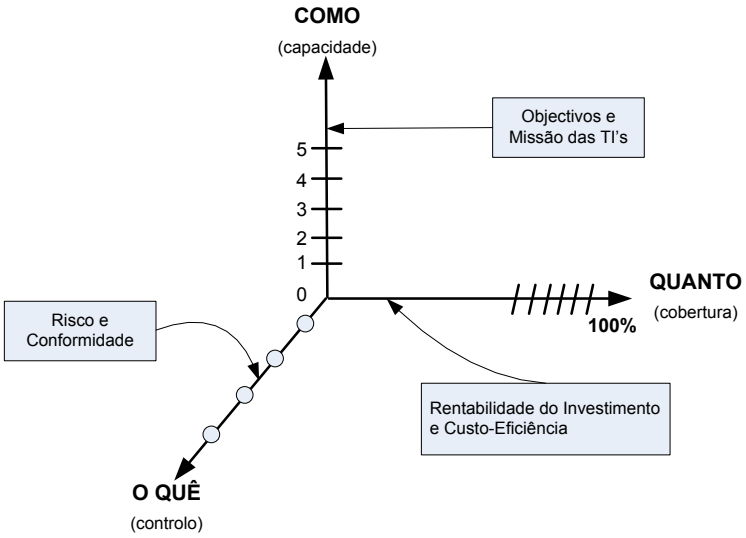
Quadro 5: Fases do modelo de maturidade do CobiT.

Nível	Descrição
0 ***Não existente***	• Não existe avaliação do risco para processos nem para as decisões do negócio. • A organização não reconhece a necessidade de implementar uma política de segurança da informação. • A organização não tem uma compreensão dos riscos, vulnerabilidades e ameaças para as operações das TIC ou o impacto das perdas ao nível dos serviços prestados pelas TIC para a continuidade das operações do negócio.
1 ***Inicial (ad hoc)***	• A organização trata os riscos das TIC de forma intermitente, sem utilizar políticas e procedimentos formais. • A organização reconhece a necessidade de implementar uma política de segurança da informação. • As responsabilidades pela continuidade dos serviços são informais e com autoridade limitada.
2 ***Repetitivo mas intuitivo***	• A organização compreende a importância dos riscos das TIC e da necessidade de os controlar e gerir. • As responsabilidades para a segurança da informação são atribuídas, mas não ao nível superior da gestão. • É atribuída responsabilidade pela continuidade do serviço.
3 ***Processos definidos***	• Existência de uma política geral de gestão do risco que define quando e como realizar a avaliação do risco. • Existe consciência sobre a problemática da segurança e a mesma é promovida pela gestão. A gestão comunica de forma consistente a necessidade da continuidade do serviço.
4 ***Gerível e mensurável***	• A avaliação do risco é um procedimento estandardizado e as excepções aos procedimentos carecem da aprovação da gestão das TIC. • As responsabilidades para a segurança da informação estão claramente atribuídas e reforçadas. • As responsabilidades e as normas para a continuidade do serviço são reforçadas.
5 ***Optimizado***	• A avaliação do risco é realizada regularmente com base nos processos definidos e gerida em conformidade. • A segurança da informação é uma responsabilidade comum da gestão das TIC e do negócio e está devidamente enquadrada com os objectivos de segurança do negócio da organização. • Os planos de continuidade do serviço e continuidade do negócio estão integrados e alinhados.

Fonte: Adaptado de ITGI (2007).

Decorrente deste modelo, constata-se que a maturidade é função de três vectores**:** capacidade (medição dos processos de gestão implementados); cobertura (capacidade utilizada); controlos (sofisticação dos controlos implementados depende da apetência ao risco da organização e dos requisitos de conformidade exigidos), conforme ilustrado pela Figura 5.

Figura 5: As três dimensões da maturidade.



Fonte: ITGI (2007, p. 19).

O sucesso da governação da segurança da informação pode ser medido através das seguintes medidas (ITGI, 2008):

- ausência de incidentes que causem problemas junto da opinião pública;

- redução do número de novas implementações que sejam adiadas devido a problemas associados à segurança da informação;

- número dos processos críticos de negócio que têm planos de continuidade adequados;

- número dos componentes da infra-estrutura crítica com monitorização automática;

- melhoria no conhecimento dos utilizadores das suas responsabilidades na segurança da informação.

O Governo da Segurança da Informação nas Empresas Portuguesas

Metodologia

O método usado para esta investigação foi um estudo empírico, utilizando-se um questionário como principal instrumento de recolha de dados.

O questionário foi dividido em duas partes. A primeira solicita informação acerca da empresa (n.º de empregados, actividade, volume de negócios) e sobre incidentes de segurança. Na segunda parte procura-se determinar qual o conhecimento que as empresas possuem sobre as normas e regulamentos sobre a segurança da informação, quais as normas que estão obrigadas por lei a respeitar e quais as normas em que se baseia o seu programa de segurança da informação. Todas estas questões são de resposta múltipla, sendo possível seleccionar, entre as alternativas apresentadas, todas as opções aplicáveis à empresa. São, ainda, apresentados dois grupos de questões onde se procura recolher informação sobre as percepções da importância das empresas estarem conformidade com as regulamentações sobre segurança da informação e sobre os principais elementos do governo da segurança da informação. Os itens relativos a estes dois tipos de questões foram ancorados numa escala ordinal de cinco níveis, de "Discordo totalmente" (1) a "Concordo totalmente" (5). Estas escalas usam cinco respostas alternativas, dado que "são suficientes especialmente no caso de perguntas que solicitam atitudes, opiniões, gostos ou graus de satisfação" (Hill & Hill, 2005, p. 124).

O desenho do questionário teve em consideração os aspectos relacionados com a estrutura, o formato, a ordem e a clareza das questões, as quais foram organizadas em secções para minimizar potenciais confusões nas respostas dos inquiridos, sendo atribuídos valores numéricos a cada uma das questões.

Recolha de dados

Os dados recolhidos para analisar o comportamento das empresas portuguesas relativamente à problemática da segurança da informação foram recolhidos durante os meses de Abril e Maio de 2011 através da administração de um questionário em versão electrónica (www.surveymonkey.com). Foi utilizada uma base de dados fornecida pela empresa Informa D&B com cerca de 5.000 endereços de correio electrónico, aos quais foi enviada uma mensagem electrónica a solicitar o preenchimento do questionário. Obtiveram-se 156 respostas válidas para análise, correspondendo a 3,12% do universo das empresas inquiridas. Esta taxa de resposta bastante baixa não é algo de muito preocupante, na medida em que elevadas taxas de não respostas a questionários são normais (Kotulic & Clark, 2004; Tomaskovic-Devey, Leiter, & Thompson 1994), especialmente quando se trata de matéria sensível como a segurança da informação. Segundo Kotulic e Clark (2004), os inquéritos sobre segurança da informação são um dos tipos de investigação mais intrusivos e há uma desconfiança geral em fornecer este tipo de informação.

Os dados foram tratados a partir do *software Statistical Package for the Social Sciences* (SPSS), versão 17.0.

Variáveis utilizadas

Para efeitos de análise bivariada foram definidas cinco variáveis (*CAE*, *incidentes*, *programa*, *conformidade* e *tipo_emp*) a partir da informação recolhida nos questionários. De forma a garantir os pressupostos para a realização do teste do Qui-Quadrado, técnica utilizada para avaliar a associação entre as variáveis, foi necessário fazer alguns ajustamentos às variáveis, designadamente:

- A variável *CAE* é composta por três níveis (agricultura e indústria; comércio; serviços), os quais resultaram da aglutinação lógica dos 19 códigos de classificação constantes do inquérito;
- A variável *tipo_emp* é composta por dois níveis (PME e grande empresa), sendo a distinção efectuada de acordo com o critério n.º de trabalhadores, ou seja, uma PME é caracterizada por possuir menos de 250 trabalhadores e as grandes empresa por terem mais do que 250 trabalhadores;
- As variáveis *incidentes*, *programa* e *conformidade* são variáveis dicotómicas.

Análise de Resultados

Da análise das principais estatísticas descritivas relativas às empresas que responderam ao inquérito constata-se que:

a) Os sectores de actividade mais representados nas respostas recolhidas são, de acordo com a Tabela 1, a indústria transformadora (18,6%), outras actividades de serviços (15,4%) e a administração pública e defesa, segurança social obrigatória.

Tabela 1: N.º de empresas por secção CAE.

Secções da CAE - Rev.3	Empresas	
	N.º	%
A - Agricultura, produção animal, caça, floresta e pesca	2	1,3%
B - Indústrias extractivas	1	0,6%
C - Indústrias transformadoras	29	18,6%
D - Electricidade, gás, vapor, água quente e fria e ar frio	3	1,9%
E - Captação, tratamento e distribuição de água; saneamento, gestão de resíduos e despoluição	6	3,8%
F - Construção	13	8,3%
G - Comércio por grosso e a retalho; reparação de veículos automóveis e motociclos	6	3,8%

H - Transportes e armazenagem	6	3,8%
I - Alojamento, restauração e similares	5	3,2%
J - Actividades de informação e de comunicação	9	5,8%
K - Actividades financeiras e de seguros	8	5,1%
L - Actividades imobiliárias	1	0,6%
M - Actividades de consultoria, científicas, técnicas e similares	12	7,7%
N - Actividades administrativas e dos serviços de apoio	3	1,9%
O - Administração Pública e Defesa; Segurança Social Obrigatória	19	12,2%
P - Educação	3	1,9%
Q - Actividades de saúde humana e apoio social	5	3,2%
R - Actividades artísticas, de espectáculos, desportivas e recreativas	1	0,6%
S - Outras actividades de serviços	24	15,4%
TOTAL	**156**	**100%**

b) Em termos de dimensão das empresas e tal como consta da Tabela 2, constata-se que as PME's representam 58,3% do total das empresas inquiridas e as grandes empresas 41,7%.

Tabela 2: Tipo de empresa.

Tipo de Empresa	**N.º**	**%**
PME	91	58,3%
Grande Empresa	65	41,7%
TOTAL	**156**	**100,0%**

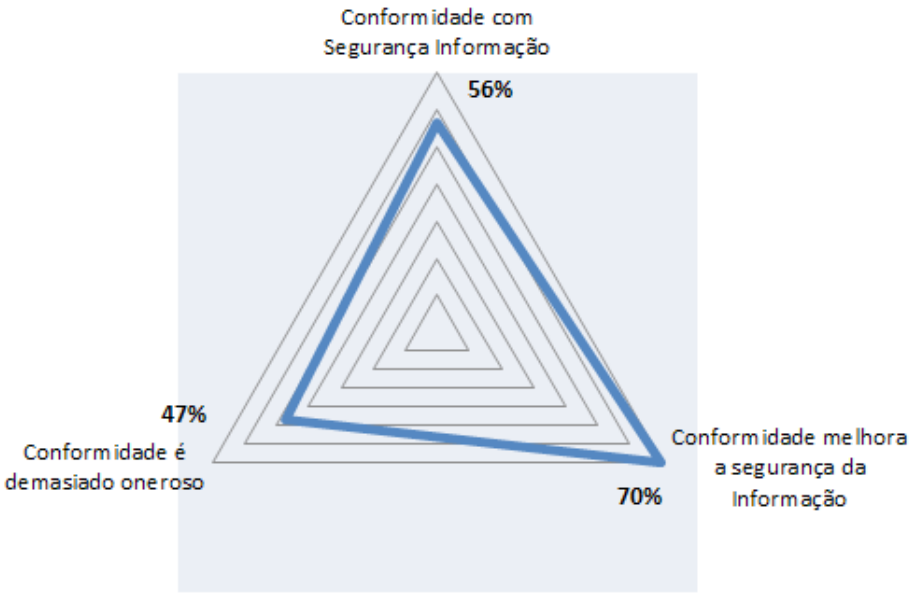
c) De acordo com a Tabela 3, cerca de 51% das empresas não sofreram nenhum incidente de segurança (nos últimos 12 meses anteriores ao momento da resposta ao inquérito), enquanto 48,7% das empresas sofreram pelo menos um incidente de segurança no mesmo período de tempo.

Tabela 3: - N.º de incidentes de segurança.

Incidentes de segurança	**N.º**	**%**
Nenhum (0)	80	51,3%
Entre 1 e 5	62	39,7%
Ente 6 e 10	8	5,1%
Mais de 10	6	3,9%
TOTAL	**156**	**100%**

Da análise às respostas relativas à forma como as empresas encaram a importância da conformidade com as regulamentações sobre segurança da informação constata-se que apenas 56% dos inquiridos afirmam que a sua organização está comprometida com a conformidade com as leis sobre segurança da informação. Todavia e conforme apresentado na Figura 6, uma maioria significativa (70%) reconhece que as obrigações regulamentares contribuem para uma melhoria da segurança da informação nas organizações e que essa conformidade não é um processo demasiado oneroso (apenas 10% assume que não é demasiado oneroso implementar uma política de conformidade sobre segurança da informação e 35% não tem percepção do custo de uma política deste tipo).

Figura 6: Aspectos mais salientes da conformidade com os regulamentos.



No que diz respeito ao conhecimento das leis, standards e regulamentos sobre segurança da informação e de acordo com a Tabela 6, apenas as leis nacionais são conhecidas por mais de 50% das empresas (tratamento de dados pessoais: 62%; protecção jurídicas das bases de dados: 59%; criminalidade informática: 54%).

Tabela 4: Leis, standards e regulamentos conhecidos pelas empresas.

Regulamento	**N.º**	**%**
Tratamento de Dados Pessoais (Lei n.º 67/98)	97	62%
Protecção Jurídica das Bases e Dados (DL 122/2000)	92	59%
Criminalidade Informática (Lei n.º 109/91)	84	54%
IT Infrastructure Library (ITIL)	53	34%
ISO/IEC 27001	45	29%
Sarbanes-Oxley Act (SOX)	32	21%
ISO/IEC 27002	32	21%
Control Objectives for Information and Related Technology (COBIT)	26	17%
Nenhum	22	14%
Normas para a Segurança Nacional Salvaguarda e Defesa das Matérias Classificadas, Segurança, Informática (SEGNAC 4)	21	13%
Basel II	17	11%
COSO	12	8%
Payment Card Industry (PCI)	11	7%
Health Insurance Portability and Accountability Act (HIPAA)	10	6%
Solvency II	6	4%
NIST SP 800 Series	5	3%

Embora existam regulamentações que as empresas estejam obrigadas a cumprir (p.e., Solvency e Basel II para as empresas de seguros e bancárias e afins; Sarbanes-Oxley Act para as empresas cotadas na bolsa de Nova Iorque), 70% dos inquiridos afirmam que a sua empresa não está obrigada por lei a estar em conformidade com nenhuma regulamentação. Das restantes empresas, cerca de 20% afirma estar em conformidade com mais do que uma regulamentação. As regulamentações que as empresas afirmam estar sujeitas são as contantes da Tabela 5.

Tabela 5: Conformidade com regulamentos.

Regulamento	**N.º**	**%**
Sarbanes-Oxley Act (SOX)	9	6%
Basel II	7	4%
ISO/IEC 27001	11	7%
ISO/IEC 27002	7	4%
Solvency II	4	3%

Relativamente à constituição do seu programa de segurança da informação, apenas 18% das empresas inquiridas não têm uma política de segurança da informação suportada em qualquer uma das regulamentações referenciadas atrás. Por outro lado, cerca de 8% das empresas baseia o seu programa de segurança da informação em mais do que uma regulamentação, com especial preponderância do COBIT, ITIL e ISO/IEC 27001/2. A Tabela 6 apresenta a estrutura das regulamentações que servem de base ao programa de segurança da informação das empresas inquiridas.

Tabela 6: Regulamentações que servem de base ao programa de segurança da informação

Regulamento	**N.º**	**%**
COBIT	31	20%
ITIL	54	35%
ISO/IEC 27001	42	27%
ISO/IEC 27002	20	13%
SEGNAC 4	5	3%
NIST SP 800 Series	3	2%
Payment Card Industry (PCI)	15	10%
Nenhum	28	18%

A percepção dos inquiridos sobre os elementos estruturantes de uma efectiva política de governo da segurança da informação revela que esses elementos não estão presentes ou existem de uma forma limitada ou insuficiente. De facto menos de 50% dos inquiridos é de opinião de que "as responsabilidades da segurança da informação estão devidamente definidas, estruturadas e documentadas", "a estratégia e os objectivos da segurança da informação estão definidos e aprovados pela administração" e que "a conformidade com a legislação, regulamentos, políticas e regras de segurança da informação é uma prioridade estratégica". Por outro lado, apenas mais de 50% tem percepção de que "os riscos da segurança da informação são geridos de forma proporcional às ameaças e ao valor dos activos" e que "os recursos da segurança da informação são utilizados de forma responsável".

Transpondo a análise dos dados para uma dimensão de determinação de associação entre variáveis, procurou-se analisar se existia alguma associação entre o sector de actividade em que a empresa se insere (variável *CAE)* e a existência de incidentes de segurança (variável incidente), existência de um programa de segurança da informação (variável programa) e a empresa estar obrigada a respeitar um regulamento de segurança (variável conformidade).

Simultaneamente, determinou-se se a dimensão da empresa (variável tipo_emp) também estava associada às três variáveis anteriores. Por último, examinou-se se existia alguma associação entre a presença de incidentes e o facto da empresa ter implementado um programa de segurança (baseado em qualquer uma das regulamentações propostas).

A análise da associação entre as variáveis em estudo foi efectuada com base no teste de independência do Qui-Quadrado, o qual produziu os resultados constantes do Quadro 6.

Quadro 6: Resultados dos testes das hipóteses.

Teste	**Teste do Qui--Quadrado**			**Coeficientes de associação**		
	Valor	**df**	***sig***	**Phi**	**C**	**V**
(*CAE / incidentes*)	1,136	2	0,567	0,085 (*sig*=0,567)	0,085 (*sig*=0,567)	0,085 (*sig*=0,567)
(*CAE / programa*)	0,917	2	0,632	0,077 (*sig*=0,632)	0,077 (*sig*=0,632)	0,077 (*sig*=0,632)
(*CAE / conformidade*)	0,789	2	0,674	0,071 (*sig*=0,674)	0,071 (*sig*=0,674)	0,071 (*sig*=0,674)
(tipo_*emp / incidentes*)	0,575	1	0,448	0,061 (*sig*=0,448)	0,061 (*sig*=0,448)	0,061 (*sig*=0,448)
(tipo_*emp / programa*)	7,959	1	0,005	0,226 (*sig*=0,005)	0,226 (*sig*=0,005)	0,220 (*sig*=0,005)
(tipo_*emp / conformidade*)	0,070	1	0,792	0,021 (*sig*=0,792)	0,021 (*sig*=0,792)	0,021 (*sig*=0,792)
(*incidentes / programa*)	3,753	1	0,053	0,155 (*sig*=0,053)	0,155 (*sig*=0,053)	0,153 (*sig*=0,053)

Da análise dos dados do Quadro 6, constata-se que não existe nenhuma associação entre o sector de actividade e as variáveis em estudo (*incidentes, programa e conformidade)*. Os valores obtidos para os respectivos testes ($\chi2 = 1,136$, df = 2, sig = 0,567; $\chi2 = 0,917$, df = 2, sig = 0,632; $\chi2 = 0,789$, df = 2, sig = 0,674) concluem pela não rejeição da hipótese nula, ou seja, de que as variáveis são independentes. De igual modo, as medidas de associação Phi, coeficiente de contingência (C) e o coeficiente V de Cramer apontam também para a ausência de relação entre as variáveis.

Relativamente à associação entre o tipo de empresa e as variáveis incidentes e conformidade, os valores obtidos para os respectivos testes ($\chi2 = 0,575$, df = 1, sig = 0,448; $\chi2 = 0,070$, df = 1, sig = 0,792) mostram que não existe qualquer tipo

de associação entre o tipo de empresa e a existência (ou não) de incidentes ou da obrigatoriedade (ou não) de estar em conformidade com normas de segurança da informação. Todavia, já é possível encontrar uma associação entre o tipo de empresa e a existência (ou não) de um programa de segurança da informação ($\chi 2 = 7{,}959$, df = 1, sig = 0,005), embora o grau de associação entre estas variáveis não seja elevado (cerca de 22%), conforme demonstrado pelos coeficientes de associação Phi, coeficiente de contingência (C) e o coeficiente V de Cramer.

Por outro lado, o teste demonstra que existe uma associação entre a existência (ou não) de incidentes e a existência (ou não) de um programa de segurança da informação ($\chi 2 = 3{,}753$, df = 1, sig = 0,053), se apenas considerarmos um erro do tipo I para $p < 0{,}10$, o que se traduz numa associação fraca (cerca de 16%) entre as variáveis, conforme traduzido pelas medidas de associação Phi, coeficiente de contingência (C) e o coeficiente V de Cramer.

Conclusões

A informação assume-se, cada vez mais, como um dos activos mais importantes das organizações, pelo que deve ser protegido contra todos os riscos e ameaças a que está sujeita. Esta protecção da informação deve ser da responsabilidade dos órgãos executivos das empresas, devendo constituir-se como parte integrante do governo da organização (Pironti, 2006; Poore, 2007; von Solms & von Solms, 2006). Nesta perspectiva, o governo da segurança da informação deve ser uma das prioridades da gestão das empresas, avaliando ameaças e riscos, definindo estratégias e alocando os recursos humanos e materiais necessários à implementação de uma adequada política de segurança da informação.

Os resultados desta investigação mostram que a maioria das empresas portuguesas não atribui muita relevância às questões relacionadas com a governação da segurança da informação. De facto, apesar de apenas 56% dos inquiridos afirmar que a sua organização está comprometida com a conformidade com as leis sobre a segurança da informação, menos de 50% dos inquiridos é que concorda que as responsabilidades da segurança da informação estão devidamente definidas, estruturadas e documentadas, que a estratégia e os objectivos da segurança da informação estão definidos e aprovados pela administração e que a conformidade com a legislação, regulamentos, políticas e regras de segurança da informação é uma prioridade estratégica.

Em consonância com estes resultados, está o facto das principais normas sobre segurança da informação apenas serem conhecidas por menos de 30% das empresas inquiridas e que 70% das empresas não são obrigadas por lei a estar em conformidade com qualquer tipo de regulamentação. Embora não tendo nenhuma influência em termos de definição e adopção de uma política de segurança, é de realçar que as principais leis nacionais associadas à segurança da informação são conhecidas por mais de 50% dos inquiridos.

Todavia, quando questionados sobre as normas que servem de base ao

seu programa de informação, constata-se que apenas 18% das empresas não suportam o seu programa de segurança da informação em qualquer das normas apresentadas.

Tendo em consideração que para Poole (2006) um modelo efectivo da segurança da informação é aquele que combina o melhor do CobiT e da ISO 17799 (predecessora da ISO 27001), os resultados desta investigação demonstram que apenas 6% das empresas utilizam estas duas normas nos seus programas de segurança da informação e que 8% baseia o seu programa em mais do que uma regulamentação em simultâneo.

Dos resultados da investigação infere-se que não existe qualquer tipo de associação entre o sector de actividade ou a dimensão da empresa e o facto da empresa ter (ou não) sofrido incidentes de segurança, ser (ou não) obrigada a estar em conformidade com alguma regulamentação e possuir (ou não) um programa de segurança da informação, exceptuando o caso de se concluir que existe uma associação, ainda que pouco elevada, entre o tipo de empresa e a presença (ou não) de um programa de segurança da informação.

Os modelos de maturidade da segurança da informação utilizam o número de incidentes como uma das medidas para avaliar o grau de sucesso do governo da segurança da informação, pelo que a ausência de incidentes de segurança pode reflectir o sucesso do programa de segurança da informação implementado na organização. Os resultados da presente investigação corroboram o postulado anterior na medida em que se demonstra que existe uma associação (ainda que fraca) entre o número de incidentes e o programa de segurança.

Em síntese, pode-se concluir que apesar da informação ser um activo crítico das organizações e que o governo da segurança da informação é o processo de gestão mais adequado para garantir que a informação esteja protegida de ameaças, as empresas portuguesas estão pouco sensibilizadas para esta problemática e a sua maioria não conhece as principais normas e regulamentações que suportam os programas de segurança da informação.

Bibliografia

ALLEN, J. H. (2005). *An Introduction to Governing for Enterprise Security*. Recuperado em 27 de Novembro, 2006, em http://www.sei.cmu.edu/publications/news-at-sei/columns/security_matters/2005/1/security-matters-2005-1.pdf.

CARALLI, R. A. (2004). *Managing for Enterprise Security (Technical Note: CMU/SEI-2004-TN-046)*. Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, Networked Systems Survivability Program. Recuperado em 8 de Maio, 2007, em http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tn046.pdf.

CARALLI, R. A. & WILSON, W. R. (2004). *The Challenges of Security*

Management. Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, Networked Systems Survivability Program. Recuperado em 31 de Agosto, 2006, em http://www.cert.org/archive/pdf/ESMchallenges.pdf.

DHILLON, G., & BACKHOUSE, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, *43*(7), 125-128. Recuperado em 3 de Julho, 2008, da Business Search Premier database.

DOHERTY, N. F., & FULFORD, H. (2006). Aligning the Information Security Policy with the Strategic Information Systems Plan. *Computers & Security*, *25*(1), 55-63. Recuperado em 26 de Junho, 2008, da b-on database.

FITZGERALD, T. (2007). Information Security Governance. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 15-34). Boca Raton: Auerbach Publications.

HILL, M. M., & HILL, A. (2005). *Investigação por Questionário (2ª ed.)*. Lisboa: Edições Sílabo.

IT GOVERNANCE INSTITUTE (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2ª ed.). Rolling Meadows: Author.

IT GOVERNANCE INSTITUTE (2007). *CobiT* 4.1. Rolling Meadows: Author.

IT GOVERNANCE INSTITUTE (2008). *Information Security Governance: Guidance for Information Security Managers*. Rolling Meadows: Author.

KNAPP, K. J., & MARSHALL, T. E. (2007). Top Management Support Essential for Effective Information Security. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 51-8). Boca Raton: Auerbach Publications.

KOTULIC, A. G., & CLARK, J. G. (2004). Why There Aren't More Information Security Research Studies. *Information & Management*, *41*(5), 597-607. Recuperado em 2 de Junho, 2007, da Business Search Premier database.

KREHNKE, D. C. (2007). Corporate Governance. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 35-44). Boca Raton: Auerbach Publications.

MOULTON, R., & COLES, R. S. (2003). Applying Information Security Governance. *Computers & Security*, *22*(7), 580-584. Recuperado em 26 de Junho,

2008, da b-on database.

NATIONAL CYBER SECURITY SUMMIT TASK FORCE. (2004). *Information Security Governance: A Call to Action*. Recuperado em 2 de Julho, 2008, em http://www.cyberpartnership.org/InfoSecGov4_04.pdf.

PIRONTI, J. P. (2006). Information Security Governance: Motivations, Benefits and Outcomes. *Information Systems Control Journal*, *4*. Recuperado em 20 de Julho, 2008, em http://www.isaca.org/Template.cfm?Section=Archives&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34036.

POOLE, V. (2006). Why Information Security Governance Is Critical to Wider Corporate Governance Demands - A European Perspective. *Information Systems Control Journal*, *1*. Recuperado em 20 de Julho, 2008, em http://www.isaca.org/Template.cfm?Section=Archives&Template=/ContentManagement/ContentDisplay.cfm&ContentID=30680.

POORE, R. S. (2007). Information Security Governance. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 89-114). Boca Raton: Auerbach Publications.

TOMASKOVIC-DEVEY, D., LEITER, J., & THOMPSON, S. (1994). Organizational Survey Nonresponse. *Administrative Science Quarterly*, *39*(3), 439-457. Recuperado em 13 de Março, 2009, da Business Source Premier database.

VON SOLMS, B. (2001). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215-218. Recuperado em 26 de Junho, 2008, da b-on database.

VON SOLMS, B. (2005). Information Security Governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104. Recuperado em 26 de Junho, 2008, da b-on database.

VON SOLMS, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security*, *24*(6), 443-447. Recuperado em 26 de Junho, 2008, da b-on database.

VON SOLMS, R., & VON SOLMS, S. H. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 108-412. Recuperado em 26 de Junho, 2008, da b-on database.

WESTBY, J. R., & ALLEN, J. H. (2007). *Governing for Enterprise Security (GES) Implementation Guide (Technical Note: CMU/SEI-2007-TN-020)*. Pittsburgh,

PA: Carnegie Mellon University, Software Engineering Institute, CERT Program. Recuperado em 11 de Maio, 2007, em http://www.sei.cmu.edu/pub/documents/07.reports/07tn020.pdf.