

Avaliação dos investimentos em segurança da informação

Joaquim A. Casaca¹

1) Instituto Superior de Línguas e Administração (ISLA Campus Lisboa), Lisboa, Portugal

joaquim.casaca@lx.isla.pt

Resumo

O investimento em segurança tem como função principal reduzir a exposição das organizações aos riscos que os seus sistemas e tecnologias de informação e comunicação estão sujeitos. Evitar um incidente de segurança é muito mais barato do que enfrentar os custos derivados desse incidente, já que os impactos provocados por um incidente de segurança podem ser devastadores para a organização.

Este artigo tem como objectivo conhecer o nível do orçamento afecto à segurança da informação nas organizações, a forma como esse investimento é percepcionado pelos gestores e se o investimento é objecto de algum tipo de avaliação e que métricas são utilizadas nessa avaliação. Esta investigação foi realizada com base num inquérito junto de 5000 empresas, tendo sido recolhidos 156 respostas válidas para análise. Os testes das hipóteses da investigação foram efectuados com base nos testes de independência do Qui-Quadrado e Kolmogorov-Smirnov.

Os resultados mostram que as despesas com a segurança da informação são consideradas como custos operacionais e não como investimento, que uma pequena parte do orçamento dos sistemas e tecnologias de informação e comunicação é afecto à segurança da informação e que o investimento em segurança da informação não é função do número de incidentes de segurança sofridos pelas organizações. Concluiu-se, ainda, que os gestores reconhecem a necessidade de estimar os benefícios resultantes deste tipo de investimento e que a sua realização deve ser justificada em termos económicos, sendo o ROI a métrica mais utilizada.

Palavras chave: investimento, segurança da informação, métricas, avaliação, informação.

1. Introdução

A segurança da informação está relacionada com a salvaguarda dos activos, os quais devem ser protegidos de ameaças através da implementação de controlos de segurança que garantam a eliminação e/ou redução dos riscos para esses activos.

A segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação ([Wang 2005]; [Henning 2006]; [ISO/IEC 2005]; [Landwehr 2001]; [Peltier 2004a]; [Posthumus & von Solms 2004]; [Ross et al. 2007]; [Ryan & Ryan 2005]; [Siponen & Oinas-Kukkonen 2007]).

Os incidentes de segurança da informação são eventos imprevistos que têm uma elevada probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [ISO/IEC 2005], os quais têm origem, segundo Wiant [2005], nas vulnerabilidades dos sistemas operativos, abuso das contas ou permissões válidas de utilizadores e erros não intencionais dos utilizadores. Ao comprometer a disponibilidade, integridade e confidencialidade da informação, os incidentes de segurança podem ter consequências desastrosas nos objectivos do negócio.

Com a generalização dos sistemas e tecnologias de informação e comunicação (SI/TIC) e a difusão da Internet, existe um elevado risco de ataques, falhas e vulnerabilidades para os activos críticos e infra-estruturas das organizações [Shih & Wen 2003] que vão desde fraudes informáticas, espionagem, sabotagem, vandalismo, fogo ou inundações. Outras ameaças com resultados danosos compreendem código malicioso, pirataria informática e ataques de negação de serviço, as quais são cada vez mais comuns e incrivelmente sofisticadas [ISO/IEC 2005d].

Dado que a segurança é um custo pelo facto de se fazer negócio [Fourie 2003], ela deve ser uma preocupação dos responsáveis financeiros das organizações, apesar de ser uma das últimas funções a ser dotada de fundos financeiros para o desenvolvimento das suas actividades [Quinnild et al. 2006]. Todavia, é necessário convencer a gestão que evitar um incidente de segurança é muito mais barato do que enfrentar os custos derivados do incidente de segurança [Kadam 2007], dado que os impactos provocados por um incidente de segurança podem ser devastadores, podendo assumir uma de três formas potenciais [Tsiakis & Stephanides 2005]:

- impacto económico imediato – o custo de reparação ou substituição dos sistemas e interrupção das operações do negócio e dos fluxos de caixa;
- impacto económico de curto prazo – perda de clientes devido à incapacidade de entregar produtos ou serviços e impacto negativo na reputação da organização;
- impacto económico de longo prazo – declínio na avaliação de mercado da organização e do valor das acções no mercado de capitais.

Nesta perspectiva, deve-se ter presente que “o custo das medidas para minimizar o impacto de potenciais incidentes de segurança deve ser compatível com o impacto esperado sobre as funções normais da organização” [Anderson et al. 1994, p. 242], pelo que se deve assegurar que os riscos são mitigados a um custo adequado [Davis 2007].

Para Schechter e Smith [2003] o investimento a realizar em segurança tem que estar alinhado com o nível desejado de segurança, o qual pode ser determinado quantitativamente como o ponto em que os custos de um invasor potencial ultrapassam os benefícios do ataque.

Reconhecendo que as decisões de investimento em segurança são complicadas, Birch e McEvoy [1992] defendem que o investimento deve ser direccionado para reduzir a exposição aos riscos inerentes aos SI/TIC no contexto dos riscos gerais do negócio.

Em função do exposto, é importante conhecer:

1. Qual o nível do orçamento dos SI/TIC que é direccionado para a segurança da informação nas organizações e a forma como são percebidos esses gastos.
2. Se os investimentos em segurança da informação são objecto de algum tipo de avaliação e que métricas são utilizadas nessa avaliação.

Para tentar responder a estas questões, este artigo faz uma breve resenha da literatura relevante nesta matéria, com base na qual se constroem as hipóteses de investigação. Em seguida descreve-se a metodologia adoptada para operacionalizar o teste das hipóteses definidas. Após a análise dos dados, discutem-se os resultados e apresentam-se um conjunto de conclusões.

2. Impactos e custos

É praticamente impraticável e dispendioso eliminar todos os riscos, pelo que cada organização deve ter consciência do nível de risco que deve aceitar. Este nível razoável de aceitação do risco é o ponto óptimo onde os custos das perdas intersectam o custo de mitigar os riscos [ISACA 2007].

Os custos associados com a segurança da informação são, de uma forma geral, tratados como despesas operacionais e não como investimento de capital [Gordon & Loeb 2006], i.e., a segurança é vista como um custo ou um encargo que deve ser controlado e não como uma actividade que contribua para o sucesso, rentabilidade ou crescimento da organização [Caralli 2004] e [Dodds & Hague 2004], além de ser considerada como uma actividade centrada na tecnologia [Caralli & Wilson 2004]. Neste sentido, propõe-se a seguinte hipótese:

H1: *Os gastos com a segurança da informação são contabilizados como custos pelas organizações.*

3. Incidentes de segurança

Tendo como objectivo explicar que a opção de adiamento do investimento em segurança da informação é responsável pela predominância das falhas de segurança, Gordon et al. [2003] concluem que o nível do investimento em segurança é função da ocorrência das falhas de segurança actuais, i.e., “existe uma resposta reactiva e não proactiva relativamente a uma parte significativa dos investimentos em segurança, o que é consistente com a perspectiva das opções

reais sobre o investimento de capital” [Gordon et al. 2003, p. 6]. Trata-se, portanto, de uma abordagem do tipo “esperar para ver”, a qual, segundo os autores, é consistente com uma perspectiva económica racional para impedir falhas de segurança de uma forma rentável. Este tipo de actuação está em consonância com as conclusões de Richardson [2008] que apontam para que os valores dedicados à segurança da informação representem uma pequena parte dos orçamentos totais de SI/TIC. Nesta perspectiva, propõem-se as seguintes hipóteses:

H2: *O orçamento dedicado pelas organizações à segurança da informação representa uma pequena parcela dos seus orçamentos totais de SI/TIC.*

H3: *As organizações fazem depender o seu investimento em segurança da informação do número de incidentes de segurança sofridos.*

4. Análise custo-benefício

Peltier [2004b] defende que após a identificação dos controlos a implementar e da sua avaliação em termos da sua exequibilidade e eficácia deve ser efectuada uma análise custo-benefício que terá como objectivo determinar o impacto de implementar ou não implementar o controlo. Esta análise custo-benefício pode ser qualitativa ou quantitativa e tem como objectivo demonstrar que os custos de implementação dos controlos podem ser justificados com a redução do nível do risco [Stoneburner et al. 2002].

Gordon e Loeb [2006] salientam que a análise custo-benefício, utilizando o modelo do valor actual líquido (VAL), é um processo económico racional e sólido para planear os investimentos de capital, mas de aplicação pouco exequível na orçamentação do investimento em segurança da informação. Este facto deve-se, segundo os autores, à dificuldade em estimar os benefícios potenciais do investimento, dado que essa estimativa pressupõe a existência de informação sobre as perdas potenciais resultantes de falhas de segurança e a probabilidade de realização dessas falhas. Apesar da fraca exequibilidade desta métrica, Gordon e Loeb [2006] argumentam que a utilização do VAL pode ser encarada como uma abordagem económica ideal para a orçamentação das despesas com a segurança da informação

Por seu lado, Rodewald [2005] afirma que a análise custo-benefício é imperfeita para responder a questões como “qual o nível de orçamento que deve ser atribuído ao departamento de segurança da informação?”, e, como tal, não se devem fazer comparações entre o investimento em segurança da informação e um investimento de capital normal. Neste sentido, o autor argumenta que a métrica *Return on Investment* (ROI) é uma métrica pobre para comparar investimentos em segurança da informação com investimentos que produzem um retorno tangível. Assim, propõe-se a seguinte hipótese:

H4: *Os gestores de SI/TIC utilizam alguma forma de análise económica na orçamentação das despesas com a segurança da informação.*

5. Métricas de avaliação do investimento

Mercuri [2003] afirma que os custos associados com a segurança dos SI/TIC são muitas vezes difíceis de avaliar porque as métricas utilizadas são irrealistas. Na sua opinião, existem custos que podem ser calculados em termos monetários, tais como o roubo de informação proprietária ou fraude financeira. Outros mais difíceis de quantificar envolvem ataques de negação de serviço, vírus, código malicioso, violação de privilégios de acesso, vandalismo em equipamentos, etc.

Uma das métricas mais utilizadas para determinar o custo-benefício da segurança da informação é, segundo Gordon e Loeb [2002a], a rentabilidade do investimento em segurança (*Return on Security Investment* [ROSI]), mas, na sua opinião, existe alguma confusão e uma utilização incorrecta desta métrica. Sobre esta temática, Gordon e Loeb afirmam que a noção contabilística de rentabilidade do investimento não é válida para avaliar decisões de investimento e que, em contrapartida, a taxa de rentabilidade interna (TIR) “é a métrica apropriada para avaliar investimentos, incluindo os investimentos em segurança da informação” [Gordon & Loeb 2002a, p. 28]. Contudo, segundo os autores, não se deve tentar maximizar a TIR nos investimentos em segurança da informação porque “seleccionando o investimento em segurança com a TIR mais elevada não se maximizam os benefícios líquidos” [Gordon & Loeb 2002a, p. 30].

O conceito de RROI (*Risk-based Return on Investment*) estabelece que “é significativamente menos oneroso aceitar alguns danos dos ataques aos sistemas do que tentar impedir totalmente todos os danos” [Pinto et al. 2006, p. 18]. Para estes autores, o RROI deve ser usado para avaliar os investimentos em segurança, tendo em atenção os níveis mínimos aceites pela organização, mas não serve para seleccionar investimentos de segurança alternativos. Segundo Pinto et al. [2006], o valor actual líquido (VAL), ao considerar o tempo no valor do dinheiro, é a medida alternativa mais robusta e consistente para o ROI quando está em causa a selecção de soluções concorrentes, mas apresenta um aspecto desfavorável, na medida em que necessita de informação detalhada sobre a identificação dos custos e proveitos ao longo do tempo. Contudo, Taudes et al. [2000] afirmam que existem duas razões para que o VAL não seja utilizado na área dos SI/TIC. “Primeiro, porque os gestores pensam intuitivamente em termos de oportunidades (opções) e estas não são obtidas pela análise VAL. Segundo, porque é difícil encontrar modelos de parâmetros correctos.” [Taudes et al. 2000, p. 228].

Para Bodin et al. [2005], as metodologias económicas tradicionais são utilizadas com algum constrangimento na área da segurança da informação, dado que uma parte significativa da informação sobre segurança da informação assume um carácter qualitativo e não financeiro. Neste sentido, propõe-se a seguinte hipótese:

H5: *Os gestores de SI/TIC utilizam pelo menos uma métrica para avaliar o investimento em segurança da informação.*

6. Metodologia

6.1 Recolha de dados

Os dados recolhidos para testar as hipóteses de investigação atrás apresentadas, foram recolhidos durante os meses de Abril e Maio de 2010 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.

6.2 Variáveis utilizadas

Para testar as hipóteses apresentadas na revisão da literatura, foram definidas seis variáveis nominais e ordinais:

- sector de actividade a que a empresa pertence (*CAE*);
- função desempenhada pelo respondente (*funcao*);
- n.º de incidentes de segurança (*incidentes*);
- percentagem do orçamento de SI/TIC dedicado à segurança da informação (*orcamento*);

- contabilização das despesas relativas à segurança da informação (*despesas*);
- métricas utilizadas para avaliar o investimento em segurança da informação (*metricas*).

Foram, ainda, definidos quatro itens, ancorados numa escala ordinal de cinco níveis, de “Discordo totalmente” (1) a “Concordo totalmente” (5). As escalas utilizadas nestes itens 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]. Estes itens, cujo objectivo é determinar a forma como as organizações avaliam os seus investimentos em segurança da informação, compreendem as seguintes preposições:

- O investimento em segurança da informação é função da probabilidade de ocorrência de incidentes de segurança (*inv1*);
- A aprovação do investimento em segurança da informação exige a estimativa dos benefícios resultantes do investimento (*inv2*);
- Todos os investimentos em segurança da informação são analisados com base numa métrica financeira (*inv3*);
- Todos os investimentos em segurança da informação têm que ser justificados em termos económicos (*inv4*);

7. Resultados

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

- a) Em termos da função exercida pelo respondente e conforme a Tabela 1, 45,5% exercem funções relacionadas com a área de segurança e de sistemas de informação, 13,5% exercem funções de gestão de topo e 34,6% dos respondentes exercem outras funções não especificadas.

Função exercida	N.º	%
Administrador executivo	9	5,8%
Director de Sistemas de Informação	46	29,5%
Director de Segurança	3	1,9%
Director de Segurança da Informação	1	0,6%
Director-Geral	12	7,7%
Administrador de Sistemas	22	14,1%
Responsável de Segurança	9	5,8%
Outro	54	34,6%
TOTAL	156	100%

Tabela 1 - Função do inquirido

- b) Os sectores de actividade mais representados nas respostas recolhidas são, de acordo com a Tabela 2, a indústria transformadora (18,6%), outras actividades de serviços (15,4%) e a administração pública e defesa, segurança social obrigatória.

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%

Tabela 2 - N.º de empresas por secção CAE

- c) De acordo com a Tabela 3, 51,3% 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.

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

Tabela 3 - N.º de incidentes de segurança

Para testar as hipóteses definidas nos pontos anteriores recorreu-se, essencialmente, ao teste de independência do Qui-Quadrado e ao teste bilateral de independência de Kolmogorov-Smirnov, na medida em que as variáveis utilizadas são predominantemente variáveis qualitativas. Os resultados obtidos para cada uma das hipóteses são os constantes do Quadro 1.

Hipóteses (variáveis)	Teste do Qui-Quadrado			Coeficientes de associação		
	Valor	df	sig	Phi	C	V
H₁ (<i>funcao / despesas</i>)	4,596	4	0,331	0,178 (sig=0,331)	0,175 (sig=0,331)	0,178 (sig=0,331)
H₂ (<i>orcamento / CAE</i>)	0,890	4	0,926	0,078 (sig=0,926)	0,055 (sig=0,926)	0,078 (sig=0,926)
H₅ (<i>inv4 / metricas</i>)	26,545	4	0,000	0,429 (sig=0,000)	0,395 (sig=0,000)	0,429 (sig=0,000)
				Kendall's tau-b	Kendall's tau-c	Gamma
H₄ (<i>inv2 / inv3</i>)	23,560	4	0,000	0,322 (sig=0,000)	0,255 (sig=0,000)	0,527 (sig=0,000)
H₃ (<i>orcamento / incidentes</i>) (<i>inv1 / incidentes</i>)	0,205 0,684		1,000 0,738			

Quadro 1 – Resultados dos testes das hipóteses

Hipótese 1. A análise da variável *despesas* mostra que 61,4% dos inquiridos contabilizam as suas despesas com a segurança da informação como custos, enquanto 38,6% o fazem como investimento. No entanto, dado que alguns destes responsáveis podem não ter um conhecimento exacto acerca dos procedimentos contabilísticos realizados pelas suas organizações sobre esta temática, procurou-se analisar se o tipo de função exercida pelo respondente está relacionado com a forma de contabilização das despesas em segurança da informação. Para este efeito, realizou-se o teste de independência do Qui-Quadrado entre as variáveis *funcao* e *despesas*. De forma a garantir os pressupostos para a realização do teste do Qui-Quadrado, reagruparam-se as funções em quatro grupos. De acordo com o Quadro 1, os valores obtidos para o teste variáveis ($\chi^2 = 4,596$, $df = 4$, $sig = 0,331$) relevam 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.

Hipótese 2. A análise da variável *orcamento* permite concluir que apenas 6,9% das organizações dedicam mais de 10% do seu orçamento de SI/TIC à segurança da informação. Dos restantes

93,1% dos inquiridos, 33,1% afectam menos de 1%, 44,1% afectam entre 1 e 10% e cerca de 15,9% não sabe qual a percentagem do orçamento de SI/TIC é dedicada à segurança da informação. De forma a sustentar esta conclusão, procedeu-se à execução do teste da independência do Qui-Quadrado para determinar se existe algum tipo de associação entre o sector de actividade da empresa e o seu nível de orçamento para a segurança da informação. Para garantir os pressupostos do teste do Qui-Quadrado procedeu-se à fusão de classes em ambas as variáveis: a variável *orcamento* ficou restringida a três classes (<1%, 2 a 10% e >10%), tal como a variável *CAE* (agricultura e indústria, comércio e serviços). Como se constata no Quadro 1, o valor do teste ($\chi^2 = 0,890$, $df = 4$, $sig = 0,926$), conduz à conclusão de que não existe relação entre o nível de orçamento para a segurança da informação e o sector de actividade em que a empresa está integrada. Os valores das medidas de associação (Phi, C de Pearson e V de Cramer) conduzem a conclusões semelhantes.

Hipótese 3. Para testar esta hipótese, recorreu-se ao teste bilateral de independência de Kolmogorov-Smirnov (K-S), o qual analisa a distribuição de uma variável ordinal (*orcamento*) numa variável dicotómica (*incidentes*). Transformou-se a variável original *incidentes* (com cinco classes) numa variável dicotómica (com incidentes e sem incidentes). O valor obtido para o teste (K-S = 0,205, $sig = 1,000$), conforme o Quadro 1, permite concluir que, para qualquer erro de tipo I do analista, não se rejeita a hipótese nula, isto é, não existe relação entre o nível de orçamento para a segurança da informação e o número de incidentes de segurança sofridos pela empresa. Para reforçar a conclusão obtida com o teste anterior, decidiu-se averiguar se a percepção dos inquiridos de que o investimento em segurança da informação é função da probabilidade de ocorrência de incidentes de segurança (variável *inv1*) está relacionada com o facto de a organização sofrer ou não incidentes de segurança (variável dicotómica *incidentes*). Para testar esta premissa, recorreu-se, também, ao teste bilateral de independência K-S. Do valor obtido para o teste (K-S = 0,684, $sig = 0,738$) conclui-se, também, que não existe relação entre a percepção dos inquiridos de que o investimento em segurança da informação é função da probabilidade de ocorrência de incidentes de segurança e o número de incidentes realmente sofridos.

Hipótese 4. A análise às variáveis *inv2* e *inv3*, indica que a maioria dos inquiridos está de acordo (concorda ou concorda totalmente) que a aprovação dos investimentos em segurança da informação exige a estimativa dos benefícios resultantes do investimento (61%) e que todos os investimentos em segurança da informação têm que ser justificados em termos económicos (66%). Para garantir os pressupostos do teste do Qui-Quadrado recodificaram-se as cinco classes de cada variável em três classes: discordância, nem concordância nem discordância, concordância. de acordo com o Quadro 1, o teste de independência do Qui-Quadrado ($\chi^2 =$

23,560, $df = 4$, $sig = 0,000$) mostra que as variáveis não são independentes. As medidas de associação simétricas (Kendall's tau-b = 0,322, Kendall's tau-b = 0,255, Gamma = 0,527) evidenciam a existência de uma associação positiva (embora não muito forte) e estatisticamente significativas ($p < 0,01$).

Hipótese 5. De acordo com a análise à variável *metricas*, 50% dos inquiridos não utilizam qualquer tipo de métrica para avaliar os seus investimentos em segurança da informação. Dos restantes, 38% utilizam uma métrica e 12% utilizam mais do que uma métrica. O ROI é utilizado por cerca de 58% das empresas que utilizam métricas, seguido do VAL (34%) e da TIR (8%). De forma a verificar se a percepção dos inquiridos de que todos os investimentos em segurança da informação são analisados com base numa métrica financeira (variável *inv4*) está relacionada com o facto de a organização utilizar ou não métricas para avaliar os seus investimentos em segurança da informação (variável dicotómica *métricas*: utiliza métricas e não utiliza métricas), procedeu-se à execução do teste de independência do Qui-Quadrado. O valor obtido para o teste ($\chi^2 = 26,545$, $df = 4$, $sig = 0,000$) constante do Quadro 1, conduz à conclusão de que existe uma associação entre as variáveis. Os coeficientes de associação (Phi = 0,429, C = 0,395, V = 0,429) evidenciam a existência de uma associação positiva relativamente forte e estatisticamente significativa ($p < 0,01$).

8. Discussão e conclusões

Como defendido por Gordon e Loeb [2006], os resultados da presente investigação confirmam que a maioria das organizações contabiliza as suas despesas com a segurança da informação como custos e não como investimento. Este tipo de tratamento das despesas com a segurança da informação é independente do tipo de estrutura organizacional responsável pela segurança da informação, situação que se consubstancia numa visão redutora da segurança da informação, não a interpretando como uma função que pode acrescentar valor à organização, mas sim como uma função geradora de custos.

Nesta perspectiva, é normal e natural que as organizações afectem uma pequena parcela dos seus orçamentos de SI/TIC à área da segurança da informação. Esta situação, tal como os resultados da investigação demonstram, é transversal a todos os sectores de actividade, dado que não existe nenhuma relação entre o nível de investimento em segurança da informação e o sector de actividade da organização. Contrariamente às conclusões de Gordon et al. [2003], os resultados obtidos permitem concluir que o nível do investimento em segurança não está relacionado com o número de incidentes sofridos pelas organizações, ou seja, estas não têm uma resposta reactiva perante os incidentes de segurança.

Relativamente à problemática da análise económica dos investimentos em segurança da informação, a presente investigação conclui que os gestores reconhecem a necessidade de estimar os benefícios resultantes deste tipo de investimento e que a sua realização deve ser justificada em termos económicos. Neste sentido, grande parte das organizações utiliza métricas financeiras para avaliar o investimento em segurança da informação, sendo o ROI a métrica mais utilizada.

Embora as despesas com a segurança da informação sejam maioritariamente consideradas como custos operacionais e não como investimento, as organizações reconhecem que, tal como noutro tipo de investimento, os valores despendidos na segurança da informação devem ser devidamente justificados em termos económicos e objecto de uma avaliação financeira.

9. Referências

- Anderson, Alison, Dennis Longley, and Lam For Kwok. "Security Modelling for Organisations." Paper presented at the *the 2nd ACM Conference on Computer and Communications Security*, Fairfax, Virginia, USA 1994.
- Birch, David G.W., and Neil A. McEvoy. "Risk Analysis for Information Systems." *Journal of Information Technology (Routledge, Ltd.)* 7, no. 1 (1992): 44-53.
- Bodin, Lawrence D., Lawrence A. Gordon, and Martin P. Loeb. "Evaluating Information Security Investments Using the Analytic Hierarchy Process." *Communications of the ACM* 48, no. 2 (2005): 79-83.
- Caralli, Richard A. "The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management (Technical Report: CMU/SEI-2004-Tr-010; Esc-Tr-2004-010)." In . Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, 2004.
- Caralli, Richard A., and William R. Wilson. *The Challenges of Security Management*. Software Engineering Institute, Carnegie Mellon University, , 2004 [cited 31-08-2006]. Available from www.cert.org/archive/pdf/ESMchallenges.pdf.
- Davis, Jeffrey. "Overview of an It Corporate Security Organization." In *Information Security Handbook (Volume 1)*, edited by Harold F. Tipton and Micki Krause, 567-77. Boca Raton: Auerbach Publications, 2007.
- Dodds, Rupert, and Ian Hague. "Information Security - More Than an IT Issue?" *Chartered Accountants Journal* 83, no. 11 (2004): 56-57.
- Fourie, L. C. H. "The Management of Information Security - a South African Case Study." *South African Journal of Business Management* 34, no. 2 (2003): 19-29.
- Gordon, Lawrence A., and Martin P. Loeb. "Return on Information Security Investments: Myths Vs Realities." *Strategic Finance* 84, no. 5 (2002a): 26-31.
- Gordon, Lawrence A., and Martin P. Loeb. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security (TISSEC)* 5, no. 4 (2002b): 438-57.
- Gordon, Lawrence A., and Martin P. Loeb. "Budgeting Process for Information Security Expenditures." *Communications of the ACM* 49, no. 1 (2006): 121-25.

- Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. "Information Security Expenditures and Real Options: A Wait and See Approach." *Computer Security Journal* 19, no. 2 (2003): 1-7.
- Henning, Ronda R. "Security Engineering: It Is All About Control and Assurance Objectives." In *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues*, edited by Merrill Warkentin and Rayford B. Vaughn, 168-81. Hershey; London; Melbourne; Singapore: Idea Group Publishing, 2006.
- Hill, Manuela Magalhães, and Andrew Hill. *Investigação Por Questionário*. 2^a ed. Lisboa: Edições Sílabo, 2005.
- Information Systems Audit and Control Association. *Cism Review Manual 2008*. Rolling Meadows, 2007.
- International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). *ISO/IEC 17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management*. 2^a ed: British Standards (BSi), 2005.
- Kadam, Avinash W. "Information Security Policy Development and Implementation." *Information Systems Security* 16, no. 5 (2007): 246-56.
- Kotulic, Andrew G., and Jan Guynes Clark. "Why There Aren't More Information Security Research Studies." *Information & Management* 41, no. 5 (2004): 597-607.
- Landwehr, Carl E. "Computer Security." *International Journal of Information Security* 1, no. 1 (2001): 3-13.
- Mercuri, Rebecca T. "Analyzing Security Costs." *Communications of the ACM* 46, no. 6 (2003): 15-18.
- Peltier, Thomas R. "Developing an Enterprisewide Policy Structure." *Information Systems Security* 13, no. 1 (2004a): 44-50.
- Peltier, Thomas R. "Risk Analysis and Risk Management." *Information Systems Security* 13, no. 4 (2004b): 44-56.
- Pinto, C. Ariel, Ashish Arora, Dennis Hall, and Edward Schmitz. "Challenges to Sustainable Risk Management: Case Example in Information Network Security." *Engineering Management Journal* 18, no. 1 (2006): 17-23.
- Posthumus, Shaun, and Rossouw von Solms. "A Framework for the Governance of Information Security." *Computers & Security* 23, no. 8 (2004): 638-46.
- Quinnild, James, Jeff Fusile, and Cindy Smith. "Why Information Security Belongs on the CFO's Agenda." *HFM (Healthcare Financial Management)* 60, no. 2 (2006): 56-59.
- Richardson, Robert. *2007 CSI Computer Crime and Security Survey*. Computer Security Institute, , 2008 [cited 20-05-2008]. Available from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>.
- Rodewald, Gus. "Aligning Information Security Investments With a Firm's Risk Tolerance." Paper presented at the *2nd annual conference on Information security curriculum development*, Kennesaw, Georgia 2005.
- Ross, Ron, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers. *Recommended Security Controls for Federal Information Systems (Special Publication 800-53 Revision 2)*. National Institute of Standards and Technology, , 2007 [cited 18-05-2008 . Available from <http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>.

- Ryan, Julie J. C. H., and Daniel J. Ryan. "Proportional Hazards in Information Security." *Risk Analysis: An International Journal* 25, no. 1 (2005): 141-49.
- Schechter, E., Stuart, and Michael D. Smith. "How Much Security Is Enough to Stop a Thief? the Economics of Outsider Theft Via Computer Systems and Networks." Paper presented at the *Financial Cryptography Conference*, Le Gosier, Guadalupe 2003.
- Shih, Stephen C., and H. Joseph Wen. "Building E-Enterprise Security: A Business View." *Information Systems Security* 12, no. 4 (2003): 41-49.
- Siponen, and Harri Oinas-Kukkonen. "A Review of Information Security Issues and Respective Research Contributions." *ACM SIGMIS Database* 38, no. 1 (2007): 60-80.
- Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems (Special Publication 800-30)*. National Institute of Standards and Technology, , 2002 [cited 13 de Junho 2007]. Available from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
- Taudes, Alfred, Markus Feurstein, and Andreas Mild. "Options Analysis of Software Platform Decisions: A Case Study." *MIS Quarterly* 24, no. 2 (2000): 227-43.
- Tomaskovic-Devey, Donald, Jeffrey Leiter, and Shealy1 Thompson. "Organizational Survey Nonresponse." *Administrative Science Quarterly* 39, no. 3 (1994): 439-57.
- Tsiakis, Theodosios, and George Stephanides. "The Economic Approach of Information Security." *Computers & Security* 24, no. 2 (2005): 105-08.
- Wang, Andy Ju An. "Information Security Models and Metrics." Paper presented at the *ACM Southeast Regional Conference*, Kennesaw, Georgia 2005.
- Wiant, Terry L. "Information Security Policy's Impact on Reporting Security Incidents." *Computers & Security* 24, no. 6 (2005): 448-59.