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

# Porque é necessária a segurança da informação? : da estratégia às políticas de segurança

http://hdl.handle.net/11067/1011
https://doi.org/10.34628/5mq9-6a13

# PORQUE É NECESSÁRIA A SEGURANÇA DA INFORMAÇÃO? DA ESTRATÉGIA ÀS POLÍTICAS DE SEGURANÇA.

**Joaquim António Casaca**
*joaquim.casaca@netcabo.pt*
**Manuela Faia Correia**
*Professora associada da Universidade Lusíada de Lisboa*
*mcorreia@lis.ulusiada.pt*

**Resumo**: As organizações estão sujeitas a um número cada vez maior de ameaças aos seus activos de informação, desde fraudes informáticas a sabotagem, vandalismo ou espionagem. Este artigo tem como objectivo demonstrar que a protecção dos activos de informação depende da definição de uma estratégia global de segurança, consubstanciada num conjunto de políticas, normas e procedimentos de segurança, necessários para implementar os controlos que permitam eliminar ou reduzir os riscos das ameaças que pendem sobre esses activos. Parte-se da explicitação dos conceitos de segurança da informação e da respectiva importância, para a descrição das características fundamentais que devem estar presentes na definição da estratégia e das políticas de segurança, assim como nos métodos de avaliar o progresso e sucesso do programa de segurança da informação.

**Palavras Chave:** segurança da informação, estratégia, políticas de segurança, métricas, modelos de maturidade.

**Abstract:** Organizations' information assets are increasingly under numerous threats, from computer fraud to sabotage, vandalism or espionage. This article aims to demonstrate that the protection of information assets is dependent on the definition of the organization's overall security strategy. This is translated into a set of policies, standards and security procedures required to implement the controls that extinguish or reduce the risk of threats on these assets. The article begins with the explanation of information security concepts and its importance, followed by the description of the fundamental characteristics for strategy definition and security policies and finishes with the methods to assess the progress and success of the security information program,.

**Keywords:** information security, strategy, security policies, metrics, maturity models.

## Introdução

A informação é um activo que, tal como outros activos de negócio importantes, é essencial para o negócio da organização e, consequentemente,

necessita de protecção adequada (Doughty, 2003; International Organization for Standardization/International Electrotechnical Commission [ISO/IEC], 2005b), a qual depende da probabilidade da ocorrência de um risco de segurança e da amplitude do seu impacto (ITGI, 2006).

As organizações possuem diversos activos de informação que devem ser protegidos de ameaças de variados tipos, através de estratégias e políticas de segurança da informação, implementadas com base em modelos e métricas bem definidas, permitindo às organizações melhorar o seu processo de responsabilização da segurança da informação.

A segurança da informação está a atingir uma situação bastante crítica, de tal modo que faz dela um dos maiores problemas que as empresas enfrentam actualmente, devido a uma alarmante vulnerabilidade que cresce de mão dada com o aumento geométrico dos dados gerados e o modo como os utilizadores tratam esses dados (Reed, 2007). Dodds e Hague (2004) defendem que as questões de segurança apenas assumem relevo quando uma organização sofreu um ataque que comprometeu os seus sistemas e tecnologias de informação e comunicação (SI/TIC), foi objecto de fraude ou sofreu uma interrupção nas operações do negócio. Por seu lado, AlAboodi (2006) sustenta que a segurança da informação é um elemento essencial nos processos de negócios actuais e embora não deva ser uma competência básica da organização, ela deve estar presente na cultura e nos processos de negócio da organização, para que, de acordo com Anderson (2003), seja possível garantir que os riscos da informação e os controlos estão em equilíbrio.

Este artigo está estruturado do seguinte modo. A secção 2 aborda os principais conceitos relacionados com a informação e a segurança da informação. A secção 3 realça a importância da segurança da informação como parte integrante da gestão global da organização. A secção 4 descreve o papel da estratégia e das políticas de segurança como forma de proteger adequadamente os activos das organizações. A secção 5 apresenta as métricas da segurança da informação para avaliação das medidas de segurança adoptadas e a secção 6 descreve alguns modelos de maturidade para a segurança da informação. A secção 7 apresenta as conclusões.

## Informação e Segurança da Informação

O conceito de informação aplica-se ao armazenamento, comunicação, processamento ou recepção de activos de conhecimento, tais como factos, dados ou opiniões, incluindo números, gráficos ou formas narrativas, quer oral ou mantido sob qualquer meio (Information Systems Security Association [ISSA], 2003). A informação pode ser impressa ou escrita em papel, armazenada electronicamente, transmitida por correio ou utilizando meios electrónicos, visualizada em filme ou falada em conversação. "Qualquer que seja a forma que assuma ou os meios através dos quais é partilhada ou armazenada, deve ser sempre protegida de

forma apropriada" (ISO/IEC, 2005b, p. viii). "Para satisfazer os objectivos do negócio, a informação precisa de se adaptar a determinados critérios de controlo, a que o *Control Objectives for Information and related Technology* (CobiT) se refere como requisitos do negócio para a informação" (IT Governance Institute [ITGI], 2007a, p. 10).

Os recursos de informação podem ser decompostos em (ITGI, 2007a):

- dados: objectos de dados no sentido mais lato, isto é, externos e internos, estruturados e não estruturados, sons, gráficos, etc.;
- sistemas aplicacionais: conjunto dos procedimentos manuais e automatizados;
- tecnologia: engloba o hardware, sistemas operativos, sistemas de gestão de bases de dados, redes, multimédia, etc.;
- instalações: recursos para albergar e suportar os sistemas e tecnologias de informação (SI/TIC);
- pessoas: capacidades, conhecimento e produtividade do pessoal para planear, organizar, adquirir, entregar, suportar, monitorar e avaliar serviços e sistemas de informação.

A segurança da informação está relacionada com a protecção 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, tal como representado na Figura 1 sobre os conceitos e relações de segurança.

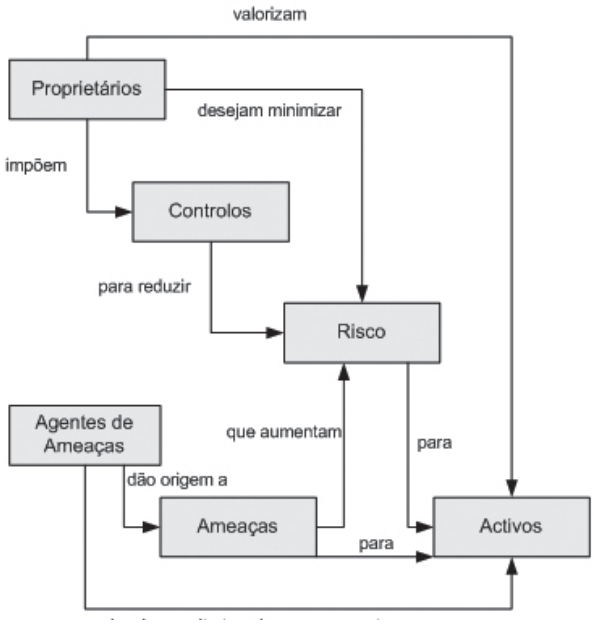


**Figura 1: Conceitos e relações de segurança.**
**Fonte: ISO/IEC (2005a, p. 12).**

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

A confidencialidade é um requisito imposto no acesso à informação em que apenas um conjunto limitado de indivíduos ou processos podem ter acesso a essa informação (Ryan & Ryan, 2005). A informação está disponível apenas aos utilizadores e/ou processos que dela necessitam, quando necessitam e sob determinadas circunstâncias (McCumber, 2005). Frequentemente, as organizações enfrentam um dilema entre a protecção da informação (confidencialidade) e a crescente necessidade de aceder a essa informação para efeitos de exploração e análise (Sarathy & Muralidhar, 2002).

A integridade da informação está relacionada com a sua exactidão e robustez, pois se a informação não é exacta ou completa pode conduzir a decisões incorrectas por parte dos gestores (Posthumus & von Solms, 2004). Uma quebra de integridade pode resultar de uma modificação intencional da informação por partes não autorizadas ou de modificação não intencional no momento do armazenamento, processamento ou transmissão (Posthumus & von Solms, 2004; Shih & Wen, 2003). Todavia, os dados podem estar disponíveis e não comprometidos relativamente à sua confidencialidade, mas estejam degradados devido a modificação ilícita (Ryan & Ryan, 2005).

A disponibilidade pretende assegurar que a informação está disponível para utilização em tempo útil (Posthumus & von Solms, 2004) e que as funções críticas são mantidas de forma contínua e que um conjunto de serviços essenciais é fornecido aos clientes (internos/externos), apesar da presença de ataques que possam comprometer a disponibilidade dos recursos da organização e imobilizar as funções normais do negócio (Shih & Wen, 2003). Sem informação atempada a organização não pode continuar com as suas operações de negócio normais. Os dados podem estar protegidos contra divulgação, modificação ilícita ou destruição, mas não estarem disponíveis quando necessários, em virtude da degradação do desempenho dos sistemas causada por um ataque de negação de serviço (Ryan & Ryan, 2005).

De acordo com o estudo de Ma, Johnston e Pearson (2008), a importância destes objectivos da segurança da informação varia em função do nível de criticidade da informação. Assim, para organizações moderamente sensíveis à informação, a confidencialidade está mais associada às práticas da gestão da segurança da informação, enquanto para as organizações altamente sensíveis à informação, a confidencialidade, a integridade e a responsabilização são os objectivos mais importantes da gestão da segurança da informação.

Outros conceitos básicos associados à segurança da informação (relacionados com a utilização da Internet) são:

- autenticação – assegurar que o utilizador é quem ele reivindica ser;
- não-repudiação – o utilizador não pode negar posteriormente que não realizou determinada actividade (Braithwaite, 2002; Landwehr, 2001);
- responsabilidade - estipular as responsabilidades e papéis dos utilizadores dos SI/TIC (Shih & Wen, 2003).

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, 2005b), 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, como esquematicamente representados na Figura 2, podem ter consequências desastrosas nos objectivos do negócio.

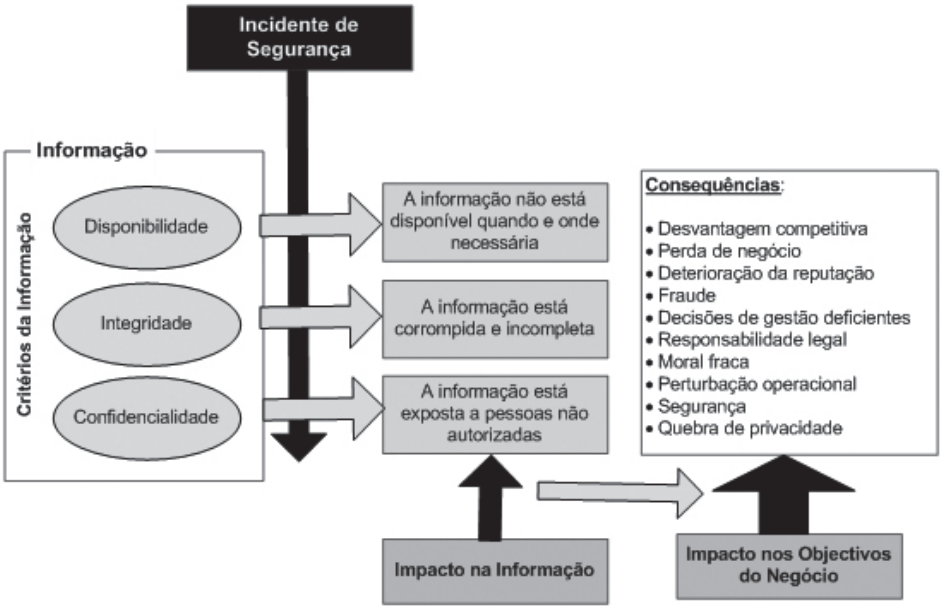


**Figura 2: Incidente de segurança.**
**Fonte: ITGI (2007b, p. 13).**

Nos últimos anos assistiu-se a alterações dramáticas na natureza e estrutura dos SI/TIC, fazendo com que as tradicionais soluções de segurança já não sejam suficientes para enfrentar os problemas de segurança actuais (Lipson & Fisher, 2000). Isto é especialmente importante num ambiente de negócio cada vez mais interligado entre clientes, fornecedores e outros parceiros de negócio. Como resultado deste incremento de interligação entre sistemas, a informação está exposta a um número e variedade crescente de ameaças e vulnerabilidades (Dhillon, Tejay, & Hong, 2007). Com a generalização dos 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, 2005b). De acordo

com o inquérito de 2007 do Computer Security Institute (CSI) (Richardson, 2008), 46% dos inquiridos afirmaram que as suas organizações sofreram um incidente de segurança nos últimos doze meses, sendo que 26% destes sofreram mais de 10 incidentes nesse período. O tipo de incidentes reportados por mais de 50% dos inquiridos dizem respeito a abusos no acesso à Internet por utilizadores internos (59%), vírus (52%) e roubo de computadores portáteis e dispositivos móveis (50%). Todos estes ataques provocaram em 2007 perdas financeiras num total de cerca de 67 milhões de dólares, dos quais 21 milhões correspondem a fraudes financeiras, oito milhões a vírus, cerca de sete milhões a penetração de sistemas por atacantes externos e cerca de seis milhões devido a roubo de dados confidenciais. Todavia, segundo o inquérito da CIO, CSO e da PriceWaterhouseCoopers (Berinato, 2007), ainda existem responsáveis pela segurança da informação que não sabem o número e natureza dos incidentes de segurança sofridos pelas suas organizações, como se pode constatar na Tabela 1.

**Tabela 1: Percentagem de inquiridos que respondem "Não sei".**

| | 2006 | 2007 | 2007 CSO/CISO |
|---|---|---|---|
| N.º de incidentes | 29% | 40% | 29% |
| Tipo de ataque | 26% | 45% | 32% |
| Primeiro método utilizado | 26% | 33% | 20% |

**Fonte: Berinato (2007, p. 5).**

Legenda: CSO - *Chief Security Officer* (responsável pela segurança)
CISO - C*hief Information Security Officer* (responsável pela segurança da informação)

As falhas de segurança são causadas, normalmente, por (ITGI, 2007b):

- ausência de processos de gestão de riscos e ameaças;
- novas vulnerabilidades originadas pela utilização de novas tecnologias;
- ausência de processos que garantam a implementação oportuna de correcções às aplicações e sistemas;
- aumento do trabalho em rede e em equipamentos sem fios;
- ausência de uma cultura de segurança;
- disciplina insuficiente na aplicação dos controlos;
- aumento dos ataques aos SI/TIC por parte de piratas informáticos, criminosos e até terroristas;
- alteração dos requisitos de segurança emanados de normas legislativas e regulatórias.

A informação tem um papel fundamental no suporte dos processos de negócio das organizações e está exposta a três elementos fundamentais (Posthumus & von Solms, 2004; Schlarman, 2001):

- tecnologia – utilizada para armazenar, processar e transmitir informação e suportar os processos;

- pessoas – que criam e utilizam a informação através de vários meios como forma de executar e suportar os processos;
- processos – que manipulam a informação para a execução de uma operação de negócio.

Cada um destes elementos representa um potencial de risco para os activos de informação das organizações e apenas através de um adequado equilíbrio entre estes três elementos se pode atingir uma efectiva segurança da informação (Anderson, 2008). Todavia, Nicastro (2007) argumenta que uma forma de se conseguir uma melhor segurança passa por uma maior focalização nas pessoas e nos processos e menos na tecnologia, designadamente através do estabelecimento de uma cultura de segurança na organização e de um adequado programa de consciencialização e formação em segurança da informação.

## A importância da segurança da informação

Apesar da maioria dos SI/TIC não terem sido desenhados para serem seguros (ISO/IEC, 2005b), Baskerville (1993) afirma que a maioria dos responsáveis pela análise e desenho dos SI/TIC não têm a intenção de projectar um sistema de informação que seja pouco seguro ou instável. Todavia, a segurança que pode ser alcançada através de meios técnicos para prevenir estas vulnerabilidades dos SI/TIC é limitada, devendo, portanto, ser utilizada uma combinação de salvaguardas técnicas e não técnicas (ITGI, 2007b; Wylder, 2007). Nesta perspectiva, Musaji (2006) advoga que a segurança da informação é alcançada através da implementação de um adequado conjunto de controlos, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controlos necessitam ser definidos, implementados, monitorizados, revistos e aperfeiçoados quando necessário para assegurar que os objectivos específicos de segurança e do negócio da organização são alcançados (ISO/IEC, 2005b). Esta nova filosofia da segurança da informação é assumida por Caralli (2004a), ao afirmar que a segurança da informação deve ser objecto de mudança de paradigma, passando-se de uma perspectiva tecnológica da segurança para um modelo de gestão organizacional, compreendendo pessoas, processos, negócio, clientes, fornecedores e parceiros, como apresentado no Quadro 2 relativo ao modelo de gestão organizacional da segurança da informação.

**Quadro 1: Modelo de gestão organizacional da segurança da informação.**

| Área | Situação Actual | Situação Futura |
|---|---|---|
| Âmbito da Segurança | Técnico | Organizacional |
| Propriedade da Segurança | Tecnologias da Informação | Organização |
| Essência da Segurança | Descontínuo e intermitente | Integrado |
| Financiamento da Segurança | Custo | Investimento |
| Orientadores da Segurança | Externo | Interno |
| Abordagem da Segurança | *Ad hoc* | Controlado |

**Fonte: Caralli (2004a, p. 6).**

Esta alteração de paradigma torna claro que a segurança da organização não resulta apenas da segurança da sua infra-estrutura tecnológica, dado que uma abordagem centrada nos factores estratégicos protege os activos e processos críticos da organização, independentemente da sua natureza e localização (Caralli & Wilson, 2004).

A segurança da informação não é um problema técnico, mas um problema de gestão (Corby, 2002; Dutta & McCrohan, 2002; Nosworthy, 2000; Schlarman, 2002; von Solms, 2001), e também um problema social e organizacional porque os SI são sistemas técnico-sociais (Laudon & Laudon, 2006) e têm que ser operados e usados pelas pessoas (Dhillon & Backhouse, 2000). Tracy (2007) também não reduz a segurança da informação a uma mera questão técnica, pois para ele, mais importante do que protecção técnica contra ameaças e vulnerabilidades é a existência de uma forte cultura de segurança em que exista incentivo e reforço do comportamento positivo. De facto, muitas vezes existem soluções técnicas para colmatar as vulnerabilidades, mas os procedimentos e responsabilidades (elementos fundamentais da política de segurança) ou não estão definidos ou não são cumpridos conforme estipulado. Assim, para Tracy (2007), o espírito da política de segurança é transposto para a prática diária da organização através do estabelecimento de uma mentalidade de segurança como forma de fazer negócio, incluir a segurança nos processos de tomada de decisão do negócio e avaliando continuamente a segurança com base em métricas fidedignas.

"A segurança da informação é a protecção da informação de uma vasta gama de ameaças de forma a assegurar a continuidade do negócio, minimizar os riscos do negócio e maximizar os retornos dos investimentos e as oportunidades de negócio" (ISO/IEC, 2005b, p. viii), combinando sistemas, operações e controlos internos (técnicos, físicos e operacionais) para garantir a confidencialidade, integridade e disponibilidade da informação (Hong, Chi, Chao, & Tang, 2003; Peltier, 1999; Posthumus & von Solms, 2004). Estas características da informação devem ser salvaguardadas através da sua classificação, permitindo, deste modo, estabelecer os níveis apropriados de protecção, pois se toda a informação é criada da mesma forma, nem toda a informação tem o mesmo valor e está sujeita aos mesmos riscos (Appleyard, 2007; Peltier, 1998; Peltier, 1999).

"A segurança da informação protege os activos de informação contra o risco de perda, descontinuidade operacional, má utilização, divulgação não autorizada, inacessibilidade e avaria" (ITGI, 2006, p. 15), pelo que um dos seus principais objectivos consiste em reduzir os impactos danosos na organização para um nível de risco aceitável. O tipo e o perfil da organização, assim como o seu negócio e os seus objectivos influenciam o nível de risco. Quanto mais elevado o ambiente competitivo da organização, mais informação é necessária para alimentar o processo de tomada de decisão e, consequentemente, maiores são os riscos de segurança (Fourie, 2003).

Partindo do princípio de que nenhum sistema é totalmente imune a ataques, falhas ou acidentes, Lipson e Fisher (2000) desenvolvem o conceito de capacidade de sobrevivência, ou seja, as condições em que os SI/TIC conseguem funcionar, considerando um nível aceitável de funcionalidade ou um período máximo de duração de inoperacionalidade aceitável. Lipson e Fisher definem sobrevivência como a capacidade dos SI/TIC cumprirem a sua missão, de forma oportuna, mesmo na presença de ataques, falhas ou acidentes, ou seja, "a existência da organização não será ameaçada seriamente pela perda de uma proporção máxima estimável dos seus recursos" (Snow, Straub, Stucke & Baskerville, 2006, p. 156). Para Masood, Sedigh-Ali e Ghafoor (2006), a sobrevivência depende da robustez da protecção do sistema, da protecção do perímetro e dos domínios da intrusão e detecção, enquanto que para Snow et al. (2006) a solução técnica para a manutenção da sobrevivência passa pela existência de um sistema fiável que garanta 100% de redundância. Contudo, Lipson e Fisher (2000) defendem que a sobrevivência não depende apenas deste tipo de controlos tecnológicos, mas, acima de tudo, de uma correcta gestão do risco, suportada por adequadas estratégias de mitigação e contingência.

Rainer, Marshall, Knapp e Montgomery (2007) chamam a atenção para o facto dos profissionais de segurança e os gestores de negócio não terem a mesma visão dos problemas de segurança, pois se os primeiros estão mais focados nos problemas técnicos, aos segundos importa mais uma perspectiva de gestão. Este latente desfasamento de interesses, designadamente o alheamento dos técnicos da segurança relativamente à missão da organização, pode traduzir-se numa dificuldade em desenvolver e implementar uma estratégia de segurança eficaz (Caralli, 2004b).

Os benefícios de uma boa segurança da informação não se restringem apenas a uma redução do risco ou uma redução no impacto se ocorrer um evento de risco. Complementarmente, uma boa segurança da informação melhora a reputação da organização, constrói e melhora a relação de confiança com os parceiros do negócio, assim como pode aumentar a eficiência na medida em que evita a perda de tempo e esforço com a recuperação de incidentes de segurança (ITGI, 2007a). De acordo com o ITGI (2008), o sucesso da segurança da informação pode ser avaliado através da:

- conformidade total ou existência de desvios mínimos relativamente aos requisitos mínimos de segurança;
- percentagem de planos e políticas existentes e documentados, incluindo

a missão da segurança da informação, visão, objectivos e códigos de conduta;
- percentagem de planos e políticas de segurança da informação comunicados a todas as partes interessadas.

Para Knapp e Marshall (2007), o suporte da gestão é uma condição essencial para a eficácia da segurança da informação, a qual também depende da formação dos utilizadores, da cultura de segurança e da relevância e aplicação das políticas de segurança.

## Estratégia e Políticas de Segurança de Informação

Se, para Purser (2004, p. 110), "a estratégia proporciona uma estrutura consistente e coerente para a melhoria e assegura que a organização se mantém focalizada nas questões mais importantes", para G. Wang (2005) a estratégia da segurança da informação deve adaptar-se aos recursos da empresa e à orientação do negócio. Neste sentido, e ainda segundo G. Wang, a estratégia da segurança da informação é um processo único para cada organização, pois os recursos e estratégias das organizações são diferentes. Para além da dependência dos objectivos estratégicos das organizações e dos recursos ao seu dispor, a estratégia da segurança da informação depende das restrições que os requisitos legais e regulamentares impõem às organizações, na medida em que as condicionam na utilização dos seus SI/TIC e da informação (Purser, 2004). Este tipo de requisitos, como por exemplo, leis sobre protecção de dados, privacidade, segredo bancário ou leis sobre a limitação do uso de mecanismos criptográficos, podem, de acordo com Purser, ter um impacto significativo na estratégia da segurança da informação.

Caralli (2004b) defende que os factores críticos de sucesso são um método eficaz para definir uma efectiva estratégia de segurança e das actividades de gestão da segurança da informação através da organização. "Os factores críticos de sucesso definem as áreas chave do desempenho que são essenciais para que a organização realize a sua missão" (Caralli, 2004b, p. 2), pelo que representam as prioridades da gestão. Ainda segundo Caralli, os factores críticos de sucesso permitem identificar os activos críticos a proteger, os requisitos de confidencialidade, integridade e disponibilidade associados a estes activos, assim como suportar uma avaliação de riscos e definir as estratégias de mitigação e contingência a estes riscos. Para Pironti (2006), a implementação de uma estratégia de segurança da informação de sucesso deve considerar os elementos críticos:

- compromisso da gestão com as iniciativas de segurança;
- conhecimento das questões de segurança pela gestão;
- planeamento da segurança da informação deve ser realizado antes da implementação de novas tecnologias;
- integração entre o negócio e a segurança da informação;

- alinhamento da segurança da informação com os objectivos da organização.

As políticas de segurança são declarações de princípios bastante vastas que representam a posição da gestão para uma área específica de controlo (Davis, 2007; Höne & Eloff, 2002), são neutras em termos tecnológicos, orientadas para os riscos, fixam instruções e procedimentos e definem penalidades e medidas preventivas se a política é transgredida (Rees, Bandyopadhyay & Spafford, 2003). As políticas de segurança incluem as intenções e prioridades tendo em vista a protecção dos SI/TIC (objectivos da segurança), juntamente com uma descrição genérica dos meios e métodos para atingir esses objectivos (Karyda, Kiountouzis & Kokolakis, 2005), além de conter os requisitos de normas e conformidade, definição de responsabilidades da gestão da segurança da informação e referência a documentos que suportam a política (Höne & Eloff, 2002; Peltier, 1999; Shaurette, 2007; Trcek, 2003).

Para Höne e Eloff (2002), os elementos essenciais de uma política de segurança da informação são:

- definição do âmbito e objectivos da segurança da informação;
- definição da segurança da informação;
- compromisso da gestão para com a segurança da informação;
- aprovação da política;
- objectivos da política e princípios da segurança da informação;
- papéis e responsabilidades;
- acções disciplinares por violação da política;
- monitorização e revisão;
- declaração de conhecimento e aceitação da política pelos utilizadores.

Se para Davis (2007, p. 569) o objectivo fundamental das políticas de segurança é "assegurar que os riscos são tratados e controlados de forma consistente em toda a organização", para Nosworthy (2000), as políticas de segurança devem atingir outros objectivos, nomeadamente:

- demonstrar o compromisso da gestão para com a segurança da informação;
- definir as linhas orientadoras da política de segurança, enquadrando-a na gestão corrente da organização;
- manter a continuidade das operações e desse modo continuar a fornecer serviços;
- proteger os activos da organização.

Para Wiant (2005), uma efectiva política de segurança pode aumentar a comunicação de incidentes de segurança (designadamente os referentes à violação informática) e da gravidade desses mesmos incidentes. Por seu lado, Karyda *et al*. (2005), assumem que a implementação e utilização de uma política de segurança dos SI/TIC numa organização deve ter em atenção, não só o quadro de referência dos indivíduos associados aos processos de segurança, mas também o contexto social onde estes ocorrem, na medida em que as decisões inerentes à formulação e implementação da política de segurança são tomadas por pessoas e dependem

da sua experiência e conhecimento, assim como dos seus objectivos e prioridades pessoais. Karyda *et al*. (2005) concluem, então, que os factores contextuais críticos para a gestão da segurança são:

- estrutura organizacional;
- cultura organizacional;
- suporte da gestão;
- existência de um órgão responsável pela formulação e implementação da política de segurança;
- programa contínuo de educação e formação em segurança;
- participação dos utilizadores na formulação da política de segurança;
- contribuição para os objectivos dos utilizadores;

Todavia, para Tompkins (2007), o requisito primordial para garantir o sucesso contínuo das políticas de segurança passa por manter a gestão informada sobre a evolução da implementação das políticas (utilizando as ferramentas de comunicação adequadas para o efeito) e, acima de tudo, obter o compromisso da gestão pela execução, controlo e monitorização da execução das políticas.

Depois de aprovada, a política de segurança deve ser disseminada pela organização a todos aqueles que são afectados pela política, o que exige uma política de comunicação adequada (Davis, 2007). Contudo, num estudo efectuado em grandes empresas do Reino Unido, Fulford e Doherty (2003) concluem que o conhecimento específico acerca da actualização, âmbito e disseminação de tais políticas no seio das organizações é bastante limitado, apesar da maioria das empresas analisadas terem implementado políticas de segurança. Segundo os autores, esta situação pode estar associada ao facto das empresas se limitarem a implementar políticas de segurança por ser uma boa prática de gestão, em vez de as transformarem numa ferramenta de trabalho para informar os colaboradores acerca das suas responsabilidades na segurança da organização.

Segundo Tracy (2007), o sucesso das políticas de segurança pode ser avaliado através de:

- resultados de auditorias de segurança;
- medidas da produtividade perdida devido a problemas com a segurança de informação;
- satisfação do utilizador com os procedimentos da segurança da informação;
- conhecimentos do utilizador acerca dos procedimentos da segurança da informação.

Uma efectiva política de segurança da informação depende da existência ou da aplicação de um determinado conjunto de factores que von Solms e von Solms (2004) intitulam de "pecados mortais" para o insucesso de um programa de segurança da informação:

1. não reconhecer a segurança da informação como uma responsabilidade da administração da organização (governo da segurança da informação);
2. não reconhecer que a segurança da informação não é um problema

técnico, mas um problema do negócio;
3. não reconhecer que a segurança da informação é uma disciplina multi-dimensional;
4. não reconhecer que a estratégia da segurança da informação deve ser implementada com base numa adequada análise de risco;
5. não compreender a importância das boas práticas internacionais na gestão da segurança da informação;
6. não compreender que uma política de segurança organizacional é essencial;
7. não conceber que a aplicação da conformidade da segurança da informação e da sua monitorização é fundamental;
8. não reconhecer a necessidade de uma apropriada estrutura para o governo da segurança da informação;
9. não reconhecer a importância capital da consciencialização da segurança da informação entre os utilizadores;
10. não disponibilizar aos gestores da segurança da informação a infra-estrutura, ferramentas e mecanismos de suporte para executar correctamente as suas responsabilidades.

A estratégia da segurança da informação inclui um conjunto de políticas, normas, procedimentos e directrizes necessários para implementar e controlar a estratégia de segurança. Segundo o ITGI (2008), as políticas e as normas são instrumentos do governo da segurança, enquanto os procedimentos e as directrizes estão relacionados com as operações. O seu grau de autoridade e valor prático variam de forma inversa, conforme apresentado na Figura 3.

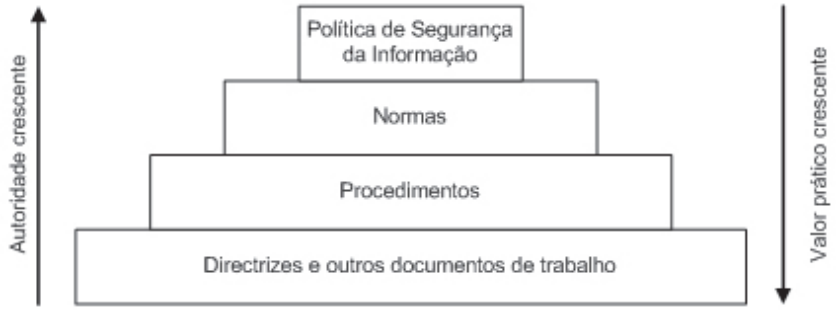


**Figura 3: Nível de autoridade e de valor das políticas, normas e procedimentos de segurança.**
**Fonte: Purser (2004, p. 134).**

No âmbito da segurança da informação, estes elementos devem ser interpretados do seguinte modo:

- políticas: são declarações de requisitos de alto nível e suficientemente gerais para serem aplicáveis em circunstâncias diversas (Purser, 2004), representando os propósitos, expectativas e orientações da administração

(ITGI, 2008; Peltier, 1999). Definem a filosofia e a postura da organização e são a base para todas as decisões e implementações de segurança subsequentes (Whitman, 2003). Devem ser em reduzido número e aprovadas pela administração, são mandatárias por natureza e são interpretadas e suportadas pelas normas, procedimentos e directrizes (Howard, 2007);

- normas: servem como especificações para a implementação das políticas (Howard, 2007; Peltier, 1999) e devem fornecer informação suficiente para que o procedimento possa ser determinado inequivocamente e respeitar os requisitos da política (ITGI, 2008). Além disso, "reduzem a complexidade, facilitam a interoperabilidade e documentam uma preferência por uma maneira particular de executar as tarefas" (Purser, 2004, p. 151). As normas devem alterar-se à medida que os requisitos e as tecnologias se vão alterando e, regra geral, devem existir várias normas para cada política, em função do domínio da segurança onde se enquadram (ITGI, 2008);
- procedimentos: definem especificamente como as políticas, normas e directrizes serão implementadas e dizem respeito a processos ou tecnologias (Howard, 2007). Devem ser inequívocas e incluir todos os passos necessários para realizar tarefas específicas (ITGI, 2008);
- directrizes: "Uma descrição de uma maneira particular de realizar algo que é menos prescritivo do que um procedimento" (ITGI, 2008, p. 45). São indicações gerais para recomendar ou sugerir uma abordagem para implementar políticas ou normas e devem conter informação que auxilie na execução dos procedimentos (Peltier, 1999).

## Métricas para a segurança da informação

O estabelecimento de metas de desempenho é um componente importante da definição das medidas da segurança da informação, pois constitui um ponto de referência para medir o sucesso, o qual é baseado na diferença entre o resultado da medição e o objectivo de desempenho declarado (Chew *et al*., 2008). Um programa de avaliação permite às organizações conhecer, gerir e melhorar o seu desempenho, na medida em que a medição efectuada permite "caracterizar, avaliar, estimar e melhorar o que está a ser produzido e a forma como é produzido" (Kasunic, McCurley & Zubrow, 2008, p. 4).

Contudo, a existência de um programa de medição e análise não está isento de erros e omissões que podem colocar em causa a própria essência e objectivos do programa. Segundo Kasunic *et al*. (2008) existem diversas fontes de erros, salientando-se as seguintes:

- ausência ou objectivos de medição confusos;
- ausência de recursos e formação;
- divergência com definições operacionais;
- falta de rigor do processo de medição;

- falta de prioridade ou interesse nas medidas e sua análise;
- erros na digitação dos dados.

Para evitar a ocorrência destes erros, Kasunic *et al*. propõem um processo de medição conforme apresentado na Figura 4.

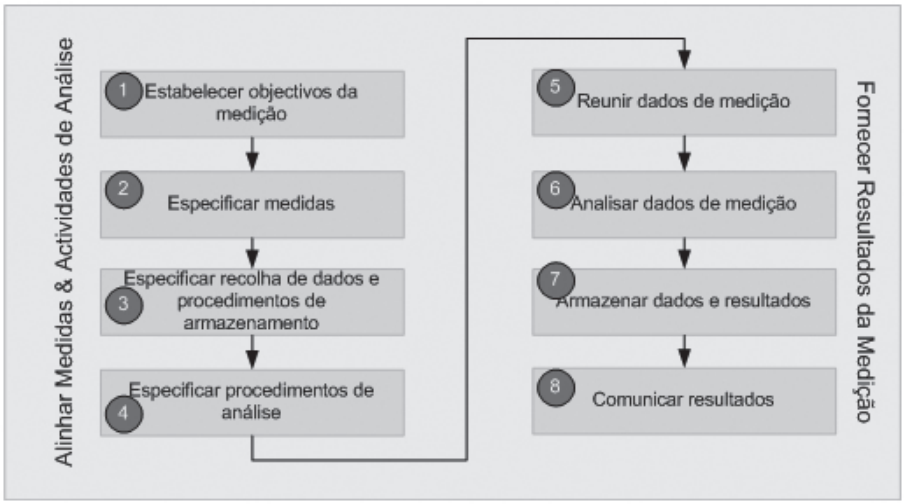


**Figura 4: Processo de medição da segurança da informação.**
**Fonte: Kasunic et al. (2008, p. 10).**

Qualquer processo de avaliação dos controlos de segurança implementados envolve um conjunto de entidades, conceitos e relações, cujo objectivo é garantir aos proprietários dos activos de informação que a avaliação realizada assegura que os controlos implementados são correctos e suficientes para minimizar os riscos dos activos, tal como expresso na Figura 5 referente aos conceitos e relações do processo de avaliação.

As métricas da segurança da informação têm como objectivo medir a eficácia dos esforços de segurança da organização ao longo do tempo (Chapin & Akridge, 2005) e podem fornecer orientação na hierarquização de acções correctivas e aumentar o nível de conhecimento da segurança na organização (Payne, 2006; A. Wang, 2005).

As métricas pretendem dar resposta a um conjunto de interrogações colocadas pelos gestores, designadamente (Chapin & Akridge, 2005):

- quais os activos que necessitam ser protegidos?
- como é que se pode justificar o custo de novos controlos de segurança?
- quando é que a organização sabe que o seu programa de segurança lhe garante um nível de segurança desejado?
- como é que a organização compara as suas práticas de segurança com as outras organizações da indústria e com as normas e melhores práticas?

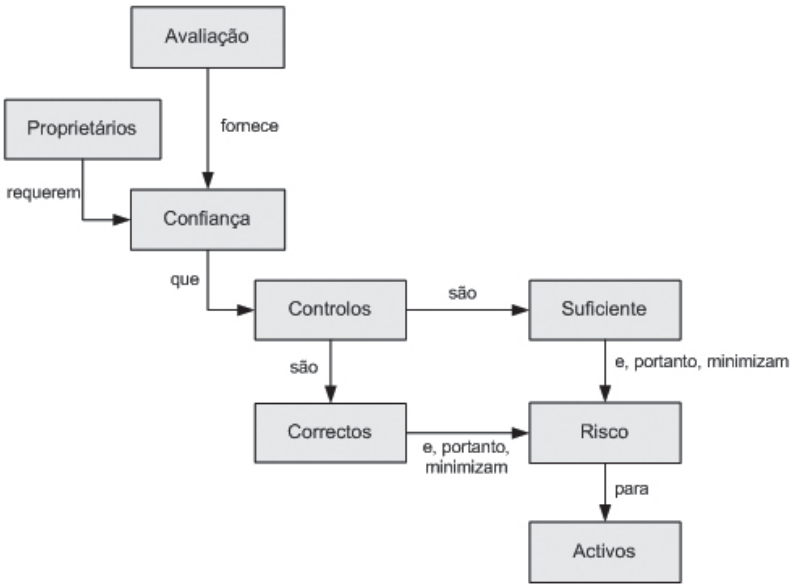


**Figura 5: Conceitos e relações do processo de avaliação.**
**Fonte: Adaptado de ISO/IEC (2005a, p. 12).**

A utilização de métricas de segurança permite às organizações melhorar o seu processo de responsabilização da segurança, pois possibilitam medir cada aspecto da organização da segurança, além de ajudarem a determinar a eficácia dos processos, procedimentos e controlos de segurança implementados (Swanson, Bartol, Sabato, Hash & Graffo, 2003).

Os benefícios da utilização de métricas de segurança podem assumir variadas formas, nomeadamente (Chew et al., 2008; Nichols & Sudbury, 2006):

- medir a eficácia dos controlos de segurança implementados;
- aumentar a responsabilidade pela segurança da informação;
- identificar áreas de segurança a melhorar;
- melhorar a eficácia da segurança de informação;
- demonstrar conformidade com leis, regulamentos;
- determinar a eficácia dos programas de gestão do risco;
- fornecer evidência de que o programa de segurança está em conformidade com as normas e melhores práticas.

As métricas de segurança devem ter as seguintes características (Chapin & Akridge, 2005; Drugescu & Etges, 2006):

- medir aspectos significativos da organização;
- serem reproduzíveis e consistentes;
- serem objectivas e imparciais;
- serem capazes de medir algum tipo de progressão relativamente a um objectivo.

Além de ter em atenção estas características das métricas, qualquer programa de avaliação da segurança da informação deve considerar os seguintes factores (Chew et al., 2008):

- as métricas devem produzir informação quantificável (números, médias, percentagens, etc.);
- os dados que suportam as métricas devem estar disponíveis no momento;
- apenas os processos de segurança da informação repetitivos devem ser considerados para avaliação;
- as métricas devem servir para acompanhar o desempenho e direccionar recursos.

A. Wang (2005) sustenta que existem alguns equívocos acerca das métricas de segurança, na medida em que estas: (i) são mais qualitativas do que quantitativas; (ii) são mais subjectivas do que objectivas; (iii) são muitas vezes definidas sem um modelo formal; (iv) não incorporam o factor tempo.

Para Payne (2006), a definição de um programa de métricas de segurança, independentemente do modelo subjacente, deve ter em consideração sete passos chave:

1. definir metas e objectivos do programa de métricas;
2. decidir as métricas a criar;
3. desenvolver modelos para a criação das métricas;
4. definir critérios de comparação;
5. estabelecer métodos para reportar as métricas;
6. criar um plano de acção para implementar as métricas;
7. estabelecer um programa contínuo de revisão e actualização das métricas.

Para Swanson *et al*. (2003) o processo de desenvolvimento das métricas de segurança dos SI/TIC compreende seis fases distintas, integradas em duas actividades principais: identificação e definição do actual programa de segurança dos SI/TIC e desenvolvimento e selecção de métricas específicas para medir a implementação, eficácia e eficiência e o impacto dos controlos de segurança, como ilustrado na Figura 6.


**Figura 6: Processo de desenvolvimento das métricas de segurança dos SI/TIC. Fonte: Swanson *et al*. (2003, p. 15).**

Swanson *et al*. (2003) definem três tipos de métricas: (1) métricas de implementação para medir a implementação da política de segurança, isto é, para demonstrar a evolução da implementação das políticas e procedimentos e nos controlos de segurança; (2) métricas de eficácia/eficiência para medir os resultados da entrega de serviços de segurança, sendo utilizadas para monitorar os resultados da implementação dos controlos de segurança; (3) métricas de impacto para medir o impacto no negócio ou na missão dos eventos e actividades de segurança, através da quantificação da poupança de custos originada pela aplicação do programa de segurança. Estas métricas podem ser utilizadas simultaneamente em qualquer programa de segurança da informação, contudo, "a utilidade das métricas varia consoante a maturidade de cada programa de segurança da informação" (Chew, Clay, Hash, Bartol & Brown, 2006, p. 15).

## Modelos de maturidade para a segurança de informação

Um dos aspectos mais importantes relacionado com as métricas é medir o progresso do programa de segurança contra um modelo de maturidade (Chapin & Akridge, 2005), pelo que se apresentam, de seguida, alguns modelos de maturidade e a sua relação com as métricas de segurança.

AlAboodi (2006) propõe um modelo de maturidade para a segurança da informação que tem como objectivo avaliar e medir a eficácia e eficiência da forma como os conceitos e práticas da segurança da informação são abordados e mantidos. Embora o autor afirme que este modelo incorpora diversas escolas de pensamento na área da segurança da informação, este modelo de maturidade está intimamente ligado à norma ISO 17799:2005, dado que existe uma ligação estreita entre os níveis do modelo e os domínios daquela norma. Trata-se de um modelo multi-nível que se propõe avaliar a "gestão da segurança da informação e a avaliação do nível da prática e consciencialização da segurança em qualquer organização assente nas tecnologias de informação e comunicação" (AlAboodi, 2006, p. 2). A utilização do modelo, representado na Figura 7, permite perceber onde e com que grau de extensão, os processos básicos da segurança (prevenção, detecção e recuperação) estão implementados e integrados.


**Figura 7: Modelo de maturidade para a segurança da informação.**
**Fonte: AlAboodi (2006, p. 2).**

As três dimensões do modelo são (AlAboodi, 2006):

- nível – o modelo apresenta cinco níveis, desde o nível 1 relativo à segurança física e ambiental até à segurança definitiva do nível 5;
- processo – diz respeito aos três processos básicos da segurança: prevenção, detecção e recuperação;
- pessoas – representa os índices sofisticação e visibilidade, os quais são apreendidos do lado das pessoas.

O National Institute of Standards and Technology [NIST] (Chew *et al*., 2006; Chew *et al*., 2008; Swanson *et al*., 2003) propõe um modelo para a maturidade do programa de segurança assente em cinco níveis:

De acordo com este modelo, esquematizado na Figura 8, o programa de segurança inicia-se pelo desenvolvimento das políticas (nível 1), pelo desenvolvimento dos procedimentos (nível 2), pela implementação dos procedimentos (nível 3), pela realização de testes de conformidade à eficácia dos procedimentos (nível 4) e, no final, pela integração total das políticas e procedimentos nas operações diárias da organização (nível 5). Os vários níveis do modelo estão associados à disponibilidade dos dados e à correspondente recolha e tratamento automático, isto é, à medida que existem mais dados disponíveis, torna-se mais fácil a sua recolha e automatização e as métricas (implementação, eficácia/eficiência e impacto) podem ser obtidas de forma mais realista.

| Disponibilidade dos Dados | Não Existente | Algum | Pode ser Recolhido | Disponível | Em Repositório Estandardizado |
|---|---|---|---|---|---|
| Dificuldade de Recolha | Muito Alto | Alto | Médio | Médio para Baixo | Baixo |
| Automatização da Recolha | Nenhum | Baixo | Médio | Alto | Completo |
| Tipos de Métricas | Definição de Objectivos | Objectivos Identificados | Implementação | Eficácia e Eficiência | Impacto |

| Desenvolvimento de Políticas | Desenvolvimento de Procedimentos | Implementação de Procedimentos e Controlos | Procedimentos e Controlos Testados | Procedimentos e Controlos Integrados |
|---|---|---|---|---|
| NÍVEL 1 | NÍVEL 2 | NÍVEL 3 | NÍVEL 4 | NÍVEL 5 |

**Figura 8: Maturidade do programa de segurança e tipos de medição.**
**Fonte: Swanson** *et al*. **(2003, p. 11).**

Após um processo de avaliação da segurança da informação é expectável que a gestão da organização execute as acções recomendadas pelos avaliadores, o que, devido a determinadas razões, nem sempre se verifica. Neal (2006) apresenta uma análise interessante sobre a resistência às conclusões da avaliação da segurança, argumentando que a resistência, entendida como uma forma passiva ou activa de não iniciar ou dar continuidade ao plano das estratégias de mitigação das ameaças identificadas numa avaliação da segurança, não é apenas função das variáveis tradicionais como riscos, restrições orçamentais, formação deficiente, má gestão ou insuficiência de recursos, mas está, também, associada a variáveis psico-sociais. Estas variáveis, segundo o autor são: o efeito espectador, controlo pessoal e incapacidade de tomar decisões, submissão à autoridade e estilo de liderança. Para eliminar o efeito destas variáveis na prossecução de um programa de segurança, Neal define um conjunto de medidas preventivas, salientando que cada uma destas medidas são "passos que a gestão pode tomar para impedir que as conclusões da avaliação possam tornar-se obsoletas e implementar as medidas de segurança necessárias para reduzir as vulnerabilidades identificadas na avaliação" (Neal, 2006, p. 51).

## Conclusões

A maioria da investigação em segurança dos SI/TIC é de natureza técnica (Dhillon & Backhouse, 2001; Dhillon & Torkzadeh, 2006), com uma atenção limitada às questões organizacionais e do factor humano, conduzindo a uma compreensão limitada da forma como as organizações gerem as várias dimensões da segurança da informação. Caralli (2004a) advoga que a segurança da informação deve ser analisada através de um modelo de gestão organizacional, compreendendo pessoas, processos, negócio, clientes, fornecedores e parceiros.

Procurando ultrapassar os aspectos técnicos da segurança da informação, este artigo aborda uma parte importante da dimensão "processos", com uma focagem nos aspectos organizacionais relativos à definição de estratégias e políticas de segurança da informação e aos processos de avaliação das medidas de controlo implementadas, designadamente as métricas e modelos de maturidade.

Em face das alterações constantes do ambiente dos SI/TIC e do surgimento diário de novas ameaças e vulnerabilidades, não basta ter uma estratégia de segurança bem definida e políticas de segurança devidamente implementadas. É necessário que as organizações sejam proactivas na avaliação contínua da segurança dos seus activos críticos, definindo um conjunto de métricas que permitam avaliar e monitorar o progresso do seu programa de segurança da informação e, simultaneamente, actualizar e reforçar continuamente as suas políticas e procedimentos de segurança.

## Bibliografia

ALABOODI, S. S. (2006). A New Approach for Assessing the Maturity of Information Security. *Information Systems Control Journal*, *3*. Recuperado em 20 de Julho, 2008, em http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=33735.

ANDERSON, J. M. (2003). Why We Need a New Definition of Information Security. *Computers & Security*, *22*(4), 308-313.

ANDERSON, K. (2008). A Business Model for Information Security. *Information Systems Control Journal*, *3*, 51-52.

APPLEYARD, J. (2007). Information Classification: A Corporate Implementation Guide. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 221-32). Boca Raton.

BASKERVILLE, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys (CSUR)*, *25*(4), 375-414.

BERINATO, S. (2007). *The Global State of Information Security 2007*. Recuperado em 21 de Maio, 2008, em www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS2007.pdf.

BRAITHWAITE, T. (2002). *Securing E-Business Systems - A Guide for Managers and Executives*. New York: John Wiley & Sons, Inc.

CARALLI, R. A. (2004a). *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. (2004b). *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management (Technical Report: CMU/SEI-2004-TR-010; ESC-TR-2004-010)* (1). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, Networked Systems Survivability Program. Recuperado em 11 de Maio, 2007, em http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr010.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.

CHAPIN, D. A., & AKRIDGE (2005). How Can Security Be Measured? *Information Systems Control Journal*, *2*. Recuperado em 30 de Julho, 2007, em http://www.isaca.org/Template.cfm?Section=Archives&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24173.

CHEW, E., CLAY, A., HASH, J., BARTOL, N., & BROWN, A. (2006). *Guide for Developing Performance Metrics for Information Security (Special Publication 800-80, Initial Public Draft)*. U.S. Department of Commerce: National Institute of Standards and Technology. Recuperado em 13 de Junho, 2007, em http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf.

CHEW, E., SWANSON, M., STINE, K., BARTOL, N., BROWN, A., & ROBINSON, W. (2008). *Performance Measurement Guide for Information Security (NIST Special Publication 800-55 Revision 1)*. U.S. Department of Commerce: National Institute of Standards and Technology. Recuperado em 25 de Novembro, 2008, em http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

CORBY, M. J. (2002). Security Is All About Business, Not Technology. *Information Systems Security*, *10*(6), 10-13.

DAVIS, J. (2007). Overview of an IT Corporate Security Organization. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6.ª ed., Vol. 1, pp. 567-77). Boca Raton: Auerbach Publications.

DHILLON, G., & BACKHOUSE, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, *43*(7), 125-128.

DHILLON, G., & BACKHOUSE, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, *11*(2), 127-143.

DHILLON, G., TEJAY, G., & HONG, W. (2007). *Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

Recuperado em 5 de Agosto, 2008, em http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2007.257.

DHILLON, G., & TORKZADEH, G. (2006). Value-focused Assessment of Information System Security in Organizations. *Information Systems Journal*, *16*(3), 293-314.

DOUGHTY, K. (2003). Implementing Enterprise Security. *Computers & Security*, *22*(2), 99-114.

DODDS, R., & HAGUE, I. (2004). Information Security - More Than an IT Issue? *Chartered Accountants Journal*, *83*(11), 56-57.

DRUGESCU, C., & ETGES, R. (2006). Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics. *Information Systems Security*, *15*(6), 30-40.

DUTTA, A., & MCCROHAN, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, *45*(1), 67-87.

FOURIE, L. C. H. (2003). The Management of Information Security - A South African Case Study. *South African Journal of Business Management*, *34*(2), 19-29.

FULFORD, H., & DOHERTY, N. F. (2003). The Application of Information Security Policies in Large UK-based Organizations: an Exploratory Investigation. *Information Management & Computer Security*, *11*(3), 106-114.

HENNING, R. R. (2006). Security Engineering: It Is All About Control and Assurance Objectives. In M. Warkentin & R. B. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (pp. 168-81). Hershey; London; Melbourne; Singapore: Idea Group Publishing.

HÖNE, K., & ELOFF, J. (2002). Information Security Policy – What do International Information Security Standards Say? *Computers & Security*, *21*(5), 402-409.

HONG, K.-S., CHI, Y.-P., CHAO, L. R., & TANG, J.-H. (2003). An Integrated System Theory of Information Security Management. *Information Management & Computer Security*, *11*(5), 243-248.

HOWARD, P. D. (2007). The Security Policy Life Cycle: Functions and Responsibilities. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 377-87). Boca Raton: Auerbach Publications.

International Organization for Standardization/ International Electrotechnical Commission. (2005a). *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*. Recuperado em 2 de Fevereiro, 2009, em http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip.

International Organization for Standardization/ International Electrotechnical Commission. (2005b). *ISO/IEC 17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management* (2ª ed.): British Standards.

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

IT Governance Institute (2007a). *CobiT* 4.1. Rolling Meadows: Author.

IT Governance Institute (2007b). *COBIT Security Baseline: An Information Security Survival Kit* (2ª ed.). Rolling Meadows: Author.

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

Information Systems Security Association. (2003). *Generally Accepted Information Security Principles (GAISP)*. Recuperado em 3 de Julho, 2008, em http://all.net/books/standards/GAISP-v30.pdf.

KARYDA, M., KIOUNTOUZIS, E., & KOKOLAKIS, S. (2005). Information Systems Security Policies: a Contextual Perspective. *Computers & Security*, *24*(3), 246-260.

KASUNIC, M., MCCURLEY, J., & ZUBROW, D. (2008). *Can You Trust Your Data? Establishing the Need for a Measurement and Analysis Infrastructure Diagnostic (Technical Note CMU/SEI-2008-TN-028)* (1): Carnegie Mellon University, Software Engineering Institute, Software Engineering Process Management Program. Recuperado em 10 de Dezembro, 2008, em http://www.sei.cmu.edu/pub/documents/08.reports/08tn028.pdf.

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.

LAUDON, K. C., & LAUDON, J. P. (2006). *Management Information Systems: Managing the Digital Firm* (9ª ed.). New Jersey: Pearson Education, Inc.

LANDWEHR, C. E. (2001). Computer Security. *International Journal of Information Security*, *1*(1), 3-13.

LIPSON, H. F., & FISHER, D. A. (2000). *Survivability - A New Technical and Business Perspective on Security*, Recuperado em 31 de Agosto, 2006, em http://www.cert.org/archive/pdf/busperspec.pdf- 401.

MA, Q., JOHNSTON, A. C., & PEARSON, J. M. (2008). Information Security Management Objectives and Practices: A Parsimonious Framework. *Information Management & Computer Security*, *16*(3), 251-270.

MASOOD, A., SEDIGH-ALI, S., & GHAFOOR, A. (2006). Security Management for an E-Enterprise. In M. Warkentin & R. B. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (pp. 95-111). Hershey; London; Melbourne; Singapore: Idea Group Publishing.

MCCUMBER, J. (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Boca Raton; London; New York; Washington, D.C.: Auerbach.

MUSAJI, Y. (2006). A Holistic Definition of IT Security - Part 1. *Information Systems Control Journal*, *3*. Recuperado em 20 de Julho, 2008, em http://www.isaca.org/Template.cfm?Section=Archives&Template=/ContentManagement/ContentDisplay.cfm&ContentID=33747.

NEAL, R. (2006). Social Psychological Variables That Contribute to Resistance to Security Assessment Findings. *Information Systems Security*, *15*(1), 43-52.

NELSON, M. (2007). Software Engineering Institute Capability Maturity Model. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 2475-89). Boca Raton: Auerbach Publications.

NICASTRO, F. M. (2007). People, Processes, and Technology: A Winning Combination. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 389-99). Boca Raton: Auerbach Publications.

NICHOLS, E. A., & SUDBURY, A. (2006). Implementing Security Metrics Initiatives. *Information Systems Security*, *15*(5), 30-38.

NOSWORTHY, J. D. (2000). Implementing Information Security in the 21st Century - Do You Have the Balancing Factors? *Computers & Security*, *19*(4), 337-347.

PAYNE, S. C. (2006). *A Guide to Security Metrics*. Recuperado em 24 de Novembro, 2008, em http://www.sans.org/reading_room/whitepapers/auditing/55.php.

PELTIER, T. R. (1998). Information Classification. *Information Systems Security*, *7*(3), 31-43.

PELTIER, T. R. (1999). *Information Security Policies and Procedures: A Practioner's Reference*. Boca Raton; London; New York; Washington, D.C.: Auerbach.

PELTIER, T. R. (2004). Developing an Enterprisewide Policy Structure. *Information Systems Security*, *13*(1), 44-50.

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.

POSTHUMUS, S., & VON SOLMS, R. (2004). A Framework for the Governance of Information Security. *Computers & Security*, *23*(8), 638-646.

PURSER, S. (2004). *A Practical Guide to Managing Information Security*. Boston; London: Artech House.

RAINER, R. K., MARSHALL, T. E., KNAPP, K. J., & MONTGOMERY, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, *16*(2), 100-108.

REED, B. (2007). Implementing Information Lifecycle Security (ILS). *Information Systems Security*, *16*(3), 177-181.

REES, J., BANDYOPADHYAY, S., & SPAFFORD, E. H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*, *46*(7), 101-106.

RICHARDSON, R. (2008). *2007 CSI Computer Crime and Security Survey*. Recuperado em 20 de Maio, 2008, em http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.

ROSS, R., KATZKE, S., JOHNSON, A., SWANSON, M., STONEBURNER, G., & ROGERS, G. (2007). *Recommended Security Controls for Federal Information Systems (Special Publication 800-53 Revision 2)*. U.S. Department of Commerce: National Institute of Standards and Technology. Recuperado em 18 de Maio, 2008, em http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf.

RYAN, J. J. C. H., & RYAN, D. J. (2005). Proportional Hazards in Information Security. *Risk Analysis: An International Journal*, *25*(1), 141-149.

SARATHY, R., & MURALIDHAR, K. (2002). The Security of Confidential Numerical Data in Databases. *Information Systems Research*, *13*(4), 389-403.

SCHLARMAN, S. (2001). The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. *Information Systems Security*, *10*(5), 36-41.

SCHLARMAN, S. (2002). The Case for a Security Information System. *Information Systems Security*, *11*(4), 44-50.

SHAURETTE, K. M. (2007). Make Security Part of Your Company's DNA. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 579-89). Boca Raton: Auerbach Publications.

SHIH, S. C., & WEN, H. J. (2003). Building E-Enterprise Security: A Business View. *Information Systems Security*, *12*(4), 41-49.

SIPONEN, M. T. & OINAS-KUKKONEN, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *ACM SIGMIS Database*, *38*(1), 60-80.

SNOW, A. P., STRAUB, D., STUCKE, C., & BASKERVILLE, R. (2006). The Survivability Principle: IT-Enabled Dispersal of Organizational Capital. In M. Warkentin & R. B. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (pp. 150-66). Hershey; London; Melbourne; Singapore: Idea Group Publishing.

SWANSON, M., BARTOL, N., SABATO, J., HASH, J., & GRAFFO, L. (2003). *Security Metrics Guide for Information Technology Systems (Special Publication 800-55)*. U.S. Department of Commerce: National Institute of Standards and Technology. Recuperado em 15 de Maio, 2007, em http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf.

TOMPKINS, W. (2007). Maintaining Management's Commitment. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 531-40). Boca Raton: Auerbach Publications.

TRACY, R. P. (2007). IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. *Information Systems Security*, *16*(2), 114-122.

TRCEK, D. (2003). An Integral Framework for Information Systems Security Management. *Computers & Security*, *22*(4), 337-360.

VON SOLMS, B. (2001). Information Security – A Multidimensional Discipline. *Computers & Security*, *20*(6), 504-508.

VON SOLMS, B., & von Solms, R. (2004). The 10 Deadly Sins of Information Security Management. *Computers & Security*, *23*(5), 371-376.

WANG, A. J. A. (2005). *Information Security Models and Metrics*. Paper presented at the ACM Southeast Regional Conference, Kennesaw, Georgia.

WANG, G. (2005). Strategies and Influence for Information Security. *Information Systems Control Journal*, *1*. Recuperado em 20 de Julho, 2008, em http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23548.

WHITMAN, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, *46*(8), 91-95.

WIANT, T. L. (2005). Information Security Policy's Impact on Reporting Security Incidents. *Computers & Security*, *24*(6), 448-459.

WYLDER, J. O. (2007). Toward Enforcing Security Policy: Encouraging Personal Accountability for Corportate Information Security Policy. In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (6ª ed., Vol. 1, pp. 367-75). Boca Raton: Auerbach Publications.