O enfoque social da segurança da informação

João Luiz Marciano
Doutorando em ciência da informação pela UnB.
E-mail: marciano@unb.br

Mamede Lima-Marques
Doutor em informatique – Universite de Toulouse III (Paul Sabatier).
E-mail: mamede@unb.br

Resumo

O uso cada vez mais disseminado de sistemas informatizados integrados por meio de redes é um fato determinante da sociedade da informação. Este universo de conteúdos e continentes digitais está sujeito a várias ameaças que comprometem seriamente a segurança do complexo usuário-sistema-informação. A tecnologia da informação é capaz de apresentar parte da solução a este problema, mas não é capaz de resolvê-lo integralmente. As políticas de segurança da informação devem contemplar o adequado equilíbrio dos aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos de políticas atuais, extremamente voltados às questões tecnológicas.

Palavras-chave

Interação social. Segurança da informação. Políticas de segurança da informação.

Social approach concerning information security

Abstract

The ever increasing use of network-integrated information systems is an Information Society's landmark. This universe of digital contents and media is prone to some threats that seriously compromise the security of the user-system-information relationship. Information technology can present part of this problem's solution, but cannot solve it integrally. The information security policies must observe the balance between the human and technology issues about information security, in contrast with current policy models, extremely devoted to technological questions.

Keywords

Information security. Information security policies. Policy networks. Social interaction.

INTRODUÇÃO

O uso cada vez amplo e disseminado de sistemas informatizados para a realização das mais diversas atividades, com a integração destes sistemas e de suas bases de dados por meio de redes, é um fato determinante da sociedade da informação. Contudo, este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário-sistema-informação. A tecnologia da informação é capaz de apresentar parte da solução a este problema, não sendo, contudo, capaz de resolvê-lo integralmente, e até mesmo contribuindo, em alguns casos, para agravá-lo. Nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas chamadas políticas de segurança da informação, que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais e de infra-estrutura e logística, além dos recursos humanos. Diante deste panorama e dada a relevância dos aspectos humanos no contexto da segurança da informação, este artigo propõe a integração de disciplinas oriundas do âmbito das ciências sociais para a construção de um arcabouço destinado à elaboração, implementação e acompanhamento de políticas de segurança abrangentes, que contemplem com o adequado equilíbrio os aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos atuais, notadamente voltados às questões tecnológicas. O roteiro apresentado propõe que se inicie a análise de tais problemas pela compreensão dos conceitos relacionados ao comportamento dos usuários dos sistemas de informação, passando pelas interações observadas neste comportamento, pela formulação do conceito do que se compreende por segurança da informação mediante esta nova conformidade e terminando com a sugestão de alguns princípios éticos e legais que venham a governá-la.

INTERAÇÃO SOCIAL E COMPORTAMENTO

As políticas de segurança da informação são, via de regra, apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adequar integralmente. Entretanto, não se vê uma discussão adequada sobre o grau de receptividade dos usuários a

estas políticas, nem se apresentam questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir (WOOD, 2000). Este artigo propõe que, antes de apresentar-se um elemento de perturbação de uma ordem vigente (mesmo que caótica), analisem-se os indivíduos e as interações ali existentes.

O campo da interação social, o qual envolve as relações intra e interorganizacionais, abarcando, por conseguinte, a gênese dos sistemas de informação ali existentes, é visto pelas diferentes ciências sob vários enfoques. A administração e a economia, por exemplo, devido à própria natureza particular dos seus objetos de estudo, debruçam-se sobre este tema com especial atenção. Da mesma forma, as estratégias de tomada de decisão e de implementação de sistemas de informação, voltadas à geração ou à manutenção de diferenciais e vantagens competitivos, ressaltam continuamente o papel preponderante assumido pelos processos de comunicação organizacional ante os demais processos presentes no ambiente analisado. A ciência da informação, por sua vez, ao ressaltar o próprio caráter transdisciplinar e o seu relacionamento com a comunicação ("a informação é um fenômeno e a comunicação é o processo de transferência ou compartilhamento deste fenômeno" (SARACEVIC, 1999)), analisa os aspectos da comunicação organizacional ora pela óptica da teoria geral dos sistemas (BATES, 1999; VON BERTALANFFY, 1975, *passim*), ora pela óptica dos processos cognitivos envolvidos na geração e na externalização desta comunicação (LIMA, 2003).

Do ponto de vista da psicologia, por sua vez, várias abordagens aos processos da comunicação têm sido apresentadas, em particular da comunicação em ambientes organizacionais, procurando afastar-se do reducionismo materialista que caracterizou tais abordagens no decorrer do século passado, especialmente em sua primeira metade (PASQUALI, 2003, pp. 19-28). Cumpre observar que as classificações apresentadas pela psicologia quanto aos aspectos comportamentais do indivíduo, em especial quanto àqueles manifestos em sua vida em sociedade e no âmbito organizacional, evoluíram da mera análise da intensidade dos processos neurais, tais como a excitação e a inibição na teoria de Pavlov, para conceitos mais elaborados baseados na resposta a estímulos vindos do meio, buscando identificar a estrutura da personalidade apresentada na resposta obtida. Esta evolução, por sua vez, veio preencher uma lacuna da teoria da administração quanto aos processos mais adequados de seleção e de colocação de pessoal e de tratamento ético de empregados em situações de demissão, entre outras necessidades. Um resultado evidente desta parceria entre psicologia e administração é a prática adotada por muitas organizações de submeter a testes psicotécnicos os candidatos a postos de trabalho ou a promoções funcionais, muitas vezes derivando para um psiquismo exacerbado (PASQUALI, 2003, pp. 29-41), em detrimento de outras análises, por exemplo socioeconômicas, que deveriam ser acrescidas ao conjunto de avaliações utilizadas.

Deve-se ressaltar, ainda, que cada um destes estudos atende a níveis específicos do ambiente organizacional: quando se quer observar o indivíduo e suas interações com o meio, utilizam-se instrumentos do campo da psicologia; quando se pretende observar o comportamento de grupos diante de situações e suas ações coletivas, recorre-se à sociologia; por fim, o estudo cultural, partindo da gênese e evolução desta cultura, é o campo da antropologia (BATES, 1999). Eis o motivo de propor-se uma análise da segurança da informação organizacional pela visão da teoria das ciências sociais: a informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é eminentemente um processo grupal, seja ela interna ou externa às fronteiras da organização.

Diversas abordagens têm sido propostas para a análise do comportamento social. A escolhida para este artigo é baseada na interação simbólica, conforme descrito a seguir.

INTERAÇÃO SIMBÓLICA E DRAMATURGIA SOCIAL

As origens da interação simbólica remetem às obras de sociólogos como Cooley, Thomas e Mead, publicadas entre o final do século XIX e o início do século XX. Este enfoque envolve a concepção da sociedade como um processo de interação, vendo-se o indivíduo e a sociedade como entidades intimamente inter-relacionadas. Além disso, dá-se especial atenção aos aspectos comportamentais do ser humano enquanto formador e mantenedor do grupo e da identidade sociais (HAGUETE, 1995, pp. 27-28). Ao referir-se à própria obra, em especial ao trabalho *Mind, Self and Society*, como pertencente ao campo do "behaviorismo social", em contraposição ao behaviorismo psicológico então dominante, Mead salientava a importância do ato social não só em termos de sua componente observável, mas também da atividade não revelada, íntima, do ato. De acordo com ele, toda atividade grupal se baseia no comportamento cooperativo, diferenciando-se o

comportamento humano pela *intenção* percebida nos atos dos demais atores e pela *resposta* baseada nesta percepção. Tais intenções são transmitidas por meio de gestos que se tornam simbólicos, portanto passíveis de serem interpretados, e que levam o homem a desenvolver a habilidade de responder aos próprios gestos. O que permite o compartilhamento de experiências e de condutas é a capacidade de diferentes seres humanos responderem da mesma forma ao mesmo gesto, desenvolvendo, assim, comportamentos grupais (HAGUETE, 1995, pp. 34).

As idéias de Mead foram revistas por vários pensadores, em especial Blumer, que em sua obra *Symbolic Interactionism, Perspective and Method*, salienta aquelas que são, em seu entendimento, as três premissas básicas do interacionismo simbólico:

1) o ser humano age com relação às coisas (todos os objetos físicos, outros seres humanos, instituições, idéias, valores) com base no sentido que elas têm para ele;

2) o *sentido* destas coisas advém da interação que o indivíduo estabelece com seu grupo social;

3) estes *sentidos* são manipulados e modificados por meio de um processo interpretativo usado pelo indivíduo ao tratar as coisas com as quais se depara.

Deste modo, o interacionismo simbólico atribui fundamental importância ao sentido que as coisas têm para o comportamento do indivíduo, além de vislumbrar este *sentido* como resultante do processo de interação entre indivíduos, e não como algo inato, constituinte da mente ou da psique. Deve-se observar a aproximação desta visão com os estudos fenomenológicos de Husserl e Merleau-Ponty, dentre outros, e com as novas abordagens da fenomenologia aplicada à ciência da informação.

Essencial para o interacionismo simbólico é também o processo de auto-interação, por meio do qual o indivíduo manipula o seu mundo e constrói sua ação (HAGUETE, 1995, pp. 29-30), seja esta ação individual ou coletiva. Contrariamente à visão então vigente de que a sociedade humana existe sob a forma de uma ordem estabelecida por meio da aderência a um conjunto de regras, normas e valores, Blumer sustenta que é o processo social de vida em grupo que cria e mantém as regras, tratando de descartar aquelas que não lhe são interessantes.

Blumer complementa que as instituições, em particular, funcionam porque as pessoas, em momentos diferentes, atuam em resposta a uma situação na qual são chamadas a agir, e não porque as organizações funcionem automaticamente em atendimento a uma dinâmica interna ou a determinado sistema de regras e requerimentos (HAGUETE, 1995, pp. 38-39).

Baseando-se na obra de Mead, Erving Gorffman, em seu trabalho mais conhecido, *The Presentation of Self in Everyday Life*, de 1959, apresenta a importância que têm as *aparências* sobre o comportamento dos indivíduos e grupos, levando-os a agir com o intento de transmitir certas impressões aos que os rodeiam, ao mesmo tempo que tentam controlar o próprio comportamento a partir das reações que lhes são transmitidas pelos demais atores, a fim de projetar uma imagem distinta da realidade. A conceituação de Gorffman envolve termos como palco, desempenho, audiência, papel, peça e ato, dentre outros do vocabulário cênico. Em termos sucintos, para Gorffman, o homem é visto não como *sendo* ou *fazendo* alguma coisa, mas sim *fingindo ser* ou *fingindo fazer* alguma coisa (HAGUETE, 1995, p. 54).

Considera-se que a análise dos temas anteriormente propostos é extremamente pertinente ao âmbito da segurança da informação, uma vez que neste âmbito é comum deparar-se com o seguinte problema: implementam-se regras (genericamente chamadas "políticas") que se mostram inadequadas ao ambiente organizacional, sendo rechaçadas pelos usuários como inadequadas, impraticáveis ou extremamente invasivas. Com o intuito de reduzir esta aversão e de contemplar questões de fato pertinentes, propõe-se a análise do comportamento dos usuários ante a segurança da informação, idealmente em dois momentos, prévia e posteriormente à adoção de tais regras.

A ANÁLISE DE COMPORTAMENTO E A FORMALIZAÇÃO DE REGRAS DE CONDUTA

A correta mensuração do comportamento individual é obtida por meio da construção, aplicação e análise de instrumentos (em geral, questionários ou entrevistas) capazes de formular de modo claro e consistente os conceitos que se deseja medir e a extensão em que se deseja medi-los. A psicologia, em suas vertentes social e comportamental, apresenta várias modalidades para a consecução de tais instrumentos, associando à aplicação destes uma gama de ferramentas estatísticas (para instrumentos quantitativos) ou de caráter analítico (para pesquisas qualitativas).

Associam-se ainda a esta discussão as idéias tecidas por Wittgenstein em suas *Considerações filosóficas*. Ali, ao falar

sobre os requisitos necessários ao entendimento de determinado contexto social, tal como a prática de seguir determinadas regras de convívio, ele afirma que este estágio implica o conhecimento ou atenção das situações subjacentes a este contexto. No entanto, para Wittgenstein, o indivíduo não pode estar ciente de todas as exigências e desdobramentos do cumprimento destas regras, permitindo a ocorrência de interpretações errôneas e ambíguas (TAYLOR, 1993).

Nestes termos, o próprio atendimento a regras é uma prática social, moldada pelos conceitos inerentes a cada indivíduo e traduzida pelas ações executadas em atendimento (ou não) às regras vigentes. Conseqüentemente, a avaliação do entendimento reside na observação das práticas adotadas, o que atribui um papel extremamente importante à compreensão do *locus* de convívio, o que se observa, por exemplo, em Merleau-Ponty, Heidegger e no próprio Wittgenstein (TAYLOR, 1993) e que se reflete no conceito de "*habitus*" (o nível de entendimento e o modo de agir social) de Bourdieu (THROOP; MURPHY, 2001). O grau com que determinada regra é aplicada reflete a sua incorporação (*embodiment*, no dizer de Merleau-Ponty) pelos indivíduos pertencentes ao contexto social do qual ela emana.

Outra indagação repousa sobre a forma de representação de tais regras: por mais que a interpretação seja moldada por experiências pessoais, esta representação deve se dar de tal modo que possa ser perceptível de maneira o mais uniforme possível por todos os que devem segui-la, evitando ambigüidades lingüísticas e reduzindo os mal-entendidos (inevitáveis, conforme já se disse, segundo Wittgenstein). Regras não são auto-aplicáveis nem autoformuláveis: elas devem ser univocamente formuladas e adequadamente aplicadas, o que exige, por vezes, elevada carga de julgamentos e percepções, tanto de seus formuladores, quanto daqueles que se espera que as sigam, além de uma prática coerentemente alinhada com a sua formulação.

No convívio social moderno, mais especificamente na sociedade da informação, a padronização de regras de conduta voltadas ao convívio diante das fontes e acervos informacionais se traduz por meio da formulação, aplicação e acompanhamento de políticas da informação, sejam elas governamentais ou organizacionais, expressas em linguagem natural, o que as sujeita a interpretações dúbias. A fim de contornar esta dificuldade, existem propostas de representar as políticas de segurança da informação com base em formalismos capazes de expressar os conceitos da linguagem natural e de averiguar a consistência dos modelos ali representados, como a lógica e, mais especificamente, as lógicas modais (GLASGOW; MACEWEN; PANANGADEN, 1992).

A ABRANGÊNCIA DA SEGURANÇA DA INFORMAÇÃO

Embora, do ponto de vista tecnológico, a necessidade de uma segurança da informação efetiva e os requisitos que almejam satisfazê-la estejam muito bem definidos e sejam amplamente conhecidos, conforme pode-se ver, por exemplo, em ABNT (2002), o estágio atual da segurança da informação assiste a um panorama no mínimo pessimista: de um lado, a engenharia de *software* propõe-se a desenvolver sistemas cuja aplicabilidade é medida quase que exclusivamente em termos práticos, atendendo-se a pressupostos do tipo "o sistema atende às finalidades para as quais foi concebido" (PRESSMAN, 1995, p. 34-36) – a este pressuposto, a segurança apresenta um adendo: "o sistema realiza as atividades para as quais foi concebido, e somente estas"; de outro, assiste-se a um número cada vez maior de ocorrências de falhas de segurança relativas a sistemas de informação que não contemplaram adequadamente os conceitos da segurança em sua formulação (SCHNEIER, 2000, p. 27).

A disseminação de meios maciços de acesso à informação, com a integração organizacional por meio da informática (FLORES et al., 1988) e posteriormente com a proliferação da internet e de redes corporativas, ao mesmo tempo que introduz formas de fácil e rápida utilização dos recursos computacionais, expõe ainda mais a fragilidade e os riscos a que estão expostos os usuários, os sistemas que utilizam e os dados armazenados e tratados por tais sistemas. Para citar-se um caso restrito ao Brasil, a iniciativa que visava à inclusão digital e que foi preconizada pelo poder público por meio do Programa Sociedade da Informação (TAKAHASHI, 2000), apontava o foco da "segurança" como essencial ao provimento de serviços de governo (vide TAKAHASHI, op. cit., p. 99). O mesmo raciocínio pode ser aplicado a outras finalidades de sistemas de informação, tais como o comércio eletrônico e o acesso a páginas de instituições financeiras por meio da internet. Em todos estes casos, a preocupação com a segurança permeia os sistemas desenvolvidos, sendo item obrigatório para a sua implementação.

Entretanto, as formas correntes de implementação de mecanismos de segurança em sistemas de informação, como a criptografia, que é utilizada como prevenção ou solução para falhas em segurança, na ampla maioria dos

casos, são notadamente técnicas, e tendem a sê-lo em grau cada vez maior, haja vista o fato de as iniciativas apresentadas se basearem em atualizações e sofisticações da tecnologia. Estas implementações incorporam elementos que, se não forem devidamente analisados, podem resultar em impactos negativos que se contrapõem e até mesmo anulam os benefícios alcançados, seja por não se incorporarem adequadamente aos sistemas de informação que os suportam, seja por trazerem consigo outras falhas inesperadas, por vezes maiores que as falhas que se tentava corrigir (SCHNEIER, 2000, p. 83). Esta abordagem da segurança da informação termina por gerar uma série de barreiras que impedem a utilização adequada e amigável dos sistemas por parte de seus usuários.

Os mecanismos de análise e de formalização de políticas de segurança atualmente em voga, tais como a norma International Organization for Standardization/ International Electrotechnical Commission – ISO/*IEC* 17799, cuja adoção no Brasil se deu por meio da norma da Associação Brasileira de Normas Técnicas (ABNT) – Norma Brasileira de Referência (NBR) 17799 (ABNT, 2002), ou a descrição de recomendações de institutos de tecnologia e de padrões, partem de pressupostos representados por "melhores práticas" (ABNT, 2002, p. 4), ou seja, adota-se um conjunto de procedimentos *ad hoc* definidos de forma empírica e exclusivamente voltados a aspectos técnicos, por vezes deslocados do contexto humano e profissional em que se inserem.

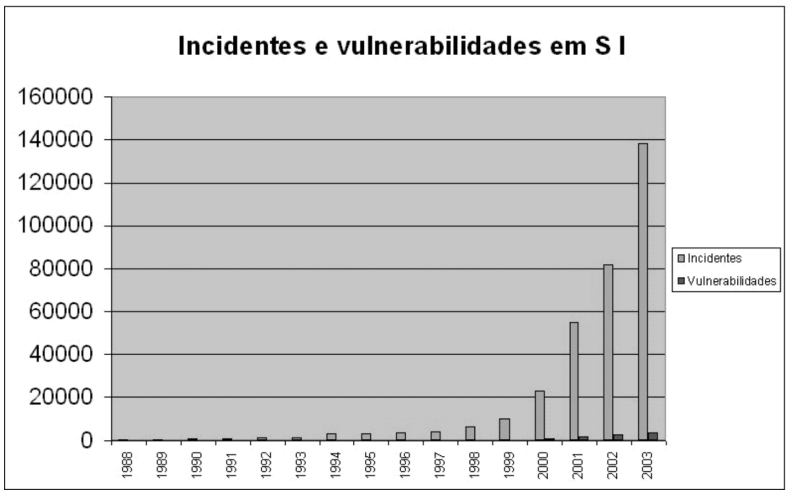
Cumpre observar que os sistemas de informação, mormente aqueles digitais, em ampla voga no contexto da sociedade da informação, encontram-se, naturalmente, envoltos por completo em ambientes do mundo real, estando sujeitos a várias formas de ações afeitas à sua segurança, tais como negações de serviço, fraudes, roubos, tentativas de invasão, corrupção e outras atividades hostis.

Em resposta a estas hostilidades, a segurança da informação, em seu sentido mais abrangente, envolve requisitos voltados à garantia de origem, uso e trânsito da informação, buscando certificar todas as etapas do seu ciclo de vida. Estes objetivos podem ser resumidos na forma dos seguintes itens (ABNT, 2002): confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade ou não repúdio.

Deste modo, a segurança se faz presente nas arquiteturas e modelos da informação, neles inserindo-se em todos os níveis. Entretanto, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação. Fraudes digitais, furtos de senhas, cavalos de tróia (códigos de programas aparentemente inofensivos, mas que guardam instruções danosas ao usuário, ao *software* ou ao equipamento), vírus e outras formas de ameaças têm se multiplicado vertiginosamente, conforme ilustra a figura 1.

Na imagem apresentada pela figura 1, mostra-se o aumento do número de vulnerabilidades, ou seja, potenciais falhas de mecanismos computacionais (implementados em *software* ou em *hardware*), as quais, uma vez exploradas, ou em virtude de fatores não-tecnológicos, como humanos, dão ensejo à ocorrência dos incidentes. Estes, por sua vez, apresentam-se em número e crescimento muito superiores às vulnerabilidades, mesmo porque a reiterada exploração da mesma vulnerabilidade pode ocasionar múltiplos incidentes. Observe-se, ainda, que um mesmo incidente que atinja diversas instalações (como a infecção por um mesmo vírus em centenas de milhares de computadores, por exemplo) é contabilizado como caso único para a confecção do gráfico. A evolução destes incidentes atesta o fato de que a tecnologia por si só, da forma como vem sendo empregada, não é capaz de solucionar semelhantes problemas, levando à ocorrência de um círculo vicioso: a aplicação da tecnologia aumenta o volume de ameaças – introduzem-se mais vulnerabilidades –, as quais procura-se combater com maior aporte tecnológico.

FIGURA 1
Vulnerabilidades e incidentes de segurança da informação em *sites* no mundo reportados no período de 1988 a 2003



Fonte: CERT (2004).

Este enfoque é resultante de uma visão canhestra da situação, que considera tão-somente os aspectos tecnológicos ali relacionados. Correntemente, para contemplar este problema a partir de uma abordagem abrangente, procede-se à adoção de estratégias organizacionais de segurança, as quais são implementadas com base em políticas de segurança institucionais.

O CONCEITO DE SEGURANÇA DA INFORMAÇÃO

A literatura especializada é pródiga na apresentação de conceitos do que a segurança da informação *faz* e de quais são os domínios de sua atuação, mas não do que ela de fato *é*. Ou seja, abundam as análises funcionais, mas são escassas as análises descritivas da segurança da informação.

Pemble (2004) sugere que a segurança da informação deve ser definida em termos das atribuições do profissional responsável por ela. O autor descreve três esferas de atuação de tais profissionais em torno das quais a segurança deveria ser parametrizada e compreendida:

- a esfera operacional, voltada ao impacto que os incidentes podem gerar à capacidade da organização de sustentar os processos do negócio;
- a esfera da reputação, voltada ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário;
- a esfera financeira, voltada aos custos em que se incorre na eventualidade de algum incidente.

Arce (2003a) lembra que diversos tipos de ataques em redes produzem resultados sobre a informação no nível semântico, ou seja, atuam sobre o significado da informação, modificando-o. A mudança de rotas de acesso em redes e a falsificação de endereços de servidores computacionais são exemplos destes ataques. Contudo, as ferramentas de detecção e prevenção atuam no nível sintático: elas tratam cadeias de caracteres em busca de padrões ou seqüências não esperadas, como é o caso de um *software* antivírus ou de uma ferramenta de prevenção de intrusões. Esta diferenciação produz um descompasso evidente entre "caça" (atacante) e "caçador" (profissional da segurança): por vezes, eles simplesmente atuam em níveis epistemológicos distintos, requerendo abordagens diferenciadas das atualmente utilizadas para a solução efetiva do problema.

Uma das frases mais citadas no contexto da segurança da informação é que "uma corrente é tão resistente quanto seu elo mais fraco". É comum a asserção de que o elo mais fraco da corrente da segurança da informação seja o usuário, uma vez que os recursos computacionais já estariam protegidos por considerável acervo tecnológico. Arce (2003b) sugere que os sistemas operacionais das estações de trabalho e seus usuários seriam os mais vulneráveis a ataques internos e externos – contudo, como já se viu, o complexo que a segurança abrange requer atenção a todos os níveis de usuários e sistemas.

Outro aspecto que se tem mostrado extremamente relevante é o custo da segurança da informação. Geer Jr, Hoo e Jaquith (2003) mostram o custo relativo para a correção de falhas de segurança em *softwares*, em cada etapa do processo de desenvolvimento, conforme ilustra a tabela 1. Como se vê, quanto mais tardiamente as falhas são detectadas e corrigidas, tanto maior é o custo em que se incorre para saná-las.

TABELA 1
Custo relativo da segurança no desenvolvimento de software

Estágio	Custo relativo
Projeto	1,0
Implementação	6,5
Testes	15,0
Manutenção	100,0

Fonte: Geer Jr, Hoo e Jaquith (2003).

Ainda, Venter e Eloff (2003) sugerem uma taxonomia para as tecnologias de segurança da informação, dividindo-as em reativas e proativas, baseando-se no clássico modelo de redes em sete camadas da Open Systems Interconnection (OSI).

Todas as definições e proposições anteriores baseiam-se ou derivam de conceitos da segurança da informação vista como um domínio tecnológico, em que ferramentas e recursos tecnológicos são aplicados em busca de soluções de problemas gerados, muitas vezes, com o concurso daquela mesma tecnologia. Evidencia-se a necessidade de uma compreensão mais abrangente destes problemas.

NECESSIDADE DE NOVO CONCEITO DE SEGURANÇA DA INFORMAÇÃO

A ausência de um conceito exato do que seja a segurança da informação já foi abordada, entre outros, por Anderson (2003). O autor cita vários textos que sugerem uma definição para o termo, mas que na verdade apresentam

as atribuições ou resultados esperados pela aplicação da segurança da informação. Ele apresenta seu próprio conceito: "Um sentimento bem fundamentado da garantia de que os controles e riscos da informação estão bem equilibrados", discorrendo em seguida sobre cada uma das partes componentes da definição.

Hitchings (1995) apresentava, já há mais de uma década, a necessidade de um conceito de segurança da informação no qual o aspecto do agente humano tivesse a devida relevância, fosse como agente ou paciente de eventos de segurança (ataques, mais especificamente).

Mesmo no aspecto tecnológico, sugestões como a de Stergiou, Leeson e Green (2004) de uma alternativa estrutural ao modelo da OSI, ou como a de Aljareh e Rossiter (2002), de um modelo de segurança colaborativo, têm sido apresentadas em contraposição ao modelo vigente.

Visto todo este contexto, propõem-se então novos conceitos, capazes de representar adequadamente os atores e o ambiente envolvidos na sistemática da segurança da informação. A primeira definição é a do que se deva entender como um sistema de informações.

> Um **sistema de informações** é composto pela somatória do sistema social no qual ele se apresenta, compreendendo os usuários e suas interações entre si e com o próprio sistema, e do complexo tecnológico sobre o qual estas interações se sustentam.

Deve-se observar que a tecnologia da informação é adotada cada vez mais como uma tecnologia de representação do mundo, real ou virtual, gerando visões próprias da realidade objetiva, as quais se estendem pela reflexividade de seu próprio uso – ou seja, a tecnologia aponta novos caminhos antes não concebidos. Assim sendo, o próprio uso da tecnologia por seus usuários constitui-se em um campo aberto a diversos questionamentos e considerações, falando-se até mesmo, como em Kim (2001), em uma fenomenologia do ser-digital. Por questões de escopo e praticidade, no presente artigo delimita-se o campo de utilização das tecnologias da informação aos ambientes organizacionais, nas esferas circunscritas pelos sistemas de informação formais, ou seja, de utilização reconhecida na organização, e utilizados com vistas aos fins organizacionais.

Entretanto, para que não pairem dúvidas sobre o tipo de usuário sobre o qual se fala, segue-se mais uma definição:

> O **usuário** de um sistema de informação é o indivíduo para o qual se concretiza o fenômeno do conhecimento mediante as informações providas por aquele sistema.

Esta definição se baseia no conceito fenomenológico de que o conhecimento representa a apropriação, por parte do indivíduo, das propriedades do objeto apresentado (HUSSERL, 1996; CAPURRO, 1982).

Não resta dúvida de que o processo de disseminação de informações por meio de redes, notadamente a internet, amplia sobremaneira o escopo de alcance dos sistemas de informação. São muitos os exemplos nos quais o alcance obtido é muito maior que o pretendido, o que nem sempre é um bom resultado.

> Segurança da informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.

Esta definição procura abranger todos os componentes localizados no complexo da segurança da informação:

1) os atores do processo (os usuários);

2) o ambiente original de sua atuação (os sistemas computacionais de informação, potencializados pelos recursos tecnológicos);

3) o alcance final dessa mesma atuação (a própria sociedade, mediante o impacto causado pelas modificações introduzidas pela utilização dos sistemas de informação).

Deste modo, tem-se uma via de mão dupla entre o contexto social no qual se inserem os sistemas de informação e a sua segurança: a partir do contexto social chega-se à definição dos requisitos necessários à segurança da informação. Em contrapartida, partindo-se dos requisitos adotados para segurança da informação, chega-se ao contexto social em que estão inseridos os sistemas – os requisitos, como regras de comportamento, refletem as interações observadas no convívio social, conforme se observou anteriormente.

Resta ainda uma questão fundamental: em que se baseiam os requisitos da segurança da informação? Em outras palavras, quais são os pressupostos necessários para

a adequada formulação de políticas de segurança da informação?

Para a correta abordagem a este problema, são apresentados alguns princípios básicos sobre os quais se propõe que se baseiem os requisitos para a formulação das políticas de segurança da informação.

PRINCÍPIOS PARA A SEGURANÇA DA INFORMAÇÃO

A correta gestão ou governança da segurança da informação é atingida com o compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos. De fato, o termo "governança" tem sido usado cada vez mais para indicar as atividades de planejamento, implementação e avaliação das atividades voltadas à segurança. Estas diferentes atividades podem ser agrupadas conforme a seguinte disposição (ISACF, 2001):

1) desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;

2) papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;

3) delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;

4) implementação, em um tempo hábil e com capacidade de manutenção;

5) monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis;

6) vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

Por sua vez, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) apresenta os seguintes princípios para o desenvolvimento de uma cultura de segurança da informação (OCDE, 2002):

1) vigilância – os participantes devem estar atentos para a necessidade da segurança dos sistemas de informação e sobre o que cada um deve fazer com vistas ao incremento desta segurança;

2) responsabilidade – todos os participantes são co-responsáveis pela segurança dos sistemas de informação;

3) responsividade – os participantes devem agir de modo coordenado e em tempo hábil a fim de prevenir, detectar e responder aos incidentes de segurança;

4) ética – cada participante deve respeitar os legítimos interesses dos demais;

5) democracia – a segurança dos sistemas de informações deve ser compatível com os valores essenciais das sociedades democráticas;

6) avaliação de risco – devem ser conduzidas avaliações de risco, periodicamente, a fim de mensurar eventuais vulnerabilidades;

7) delineamento e implementação da segurança – os participantes devem incorporar a segurança como um elemento essencial dos sistemas de informações;

8) gestão da segurança – os participantes devem adotar uma abordagem abrangente da gestão da segurança (compreendida em muitos meios como governança);

9) reavaliação – os participantes devem rever e reavaliar a segurança da informação, fazendo as modificações apropriadas a políticas, práticas, medidas e procedimentos.

Observa-se que o cumprimento de tais princípios é uma atividade discricionária, ou seja, cabe aos gestores decidir se aderem ou não às recomendações apresentadas. Pragmaticamente, cada vez mais empresas buscam a aderência a padrões internacionais ou nacionais, mesmo que advindos de fóruns externos, de segurança. No espectro governamental, há algumas imposições. Cabe menção especial à disposição da Constituição brasileira, que estabelece que

> A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência (...) (BRASIL, 2002, art. 37)

Embora estes princípios sejam comumente vistos como aplicáveis somente aos procedimentos e aos trâmites ligados às atividades da administração, como a gestão de pessoal e de finanças, não há nada que impeça a sua aplicação à segurança da informação. Pelo contrário: como os procedimentos e trâmites da administração têm

cada vez mais apoio sobre os sistemas de informação, a aplicação dos princípios dispostos pela Carta Magna a estes sistemas vem ao encontro da intenção do constituinte: garante-se que os sistemas de informação sejam aderentes aos princípios legais vigentes, de ampla utilização, atendam aos preceitos da moral e da ética, dêem vazão aos anseios democráticos por acesso à informação e atendam eficientemente aos seus objetivos.

COMENTÁRIOS FINAIS

O crescimento alarmante dos incidentes relacionados à segurança da informação alerta para a premente necessidade de uma visão fundamentada em bases sólidas para este problema, a qual extrapola em muito o âmbito da tecnologia. Esta é capaz de apresentar soluções para alguns dos problemas apresentados, mas falha clamorosamente quanto é apresentada a vários outros. Um conceito essencial a esta nova visão é o de que deve-se analisar adequadamente os papéis representados pelos usuários e suas interações diante dos sistemas de informação.

Outro aspecto que merece especial atenção é a urgente necessidade de uma discussão aprofundada dos preceitos subjacentes às políticas de segurança da informação adotadas no Brasil – em sua maioria, do lado estatal, são voltadas ao próprio aparato do Estado, salvo no tocante aos aspectos penais e judiciais. Do lado corporativo, carece-se de uma discussão adequada da realidade nacional ante o fenômeno da sociedade da informação e dos modelos que a sociedade brasileira pretende adotar diante desta realidade.

Por fim, cabe o comentário de que não se conhece qualquer solução meramente tecnológica para problemas sociais. Sendo um conceito eminentemente social, a segurança da informação necessita de uma visão igualmente embasada em conceitos sociais, além dos tecnológicos, para sua correta cobertura.

Artigo submetido em 12/06/2006 e aceito em 16/03/2007.

REFERÊNCIAS

ALJAREH, S.; ROSSITER, N. A task-based security model to facilitate collaboration in trusted multi-agency networks. In: 2002 ACM SYMPOSIUM ON APPLIED COMPUTING, 2002, Madrid. *Proceedings…* Madri: ACM, 2002. p. 744–749.

ANDERSON, J. M. Why we need a new definition of information security. *Computers & Security*, v. 22, n. 4, p. 308–313, May 2003.

ARCE, I. The rise of the gadgets. *IEEE Security & Privacy*, v. 1, n. 5, p. 78–81, Sept./Oct. 2003.

_____. The weakest link revisited. *IEEE Security & Privacy*, v. 1, n. 2, p. 72–76, Mar./Apr. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. *NBR ISO/IEC 17799*: tecnologia da informação - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

BATES, M. J. The invisible substrate of information science. *Journal of the American Society for Information Science*, v. 50, n. 12, 1999. Disponível em: <http://www.gseis.ucla.edu/faculty/bates/substrate.html>. Acesso em: 08 ago. 2003.

BRASIL. Constituição (1988). *Constituição*. Brasília: Câmara dos Deputados, Centro de Documentação e Informação, 2002.

CAPURRO, R. *Heidegger y la experiencia del lenguaje*. 1982. Disponível em: <http://www.capurro.de/boss.htm>. Acesso em: 24 maio 2005.

COMPUTER EMERGENCY RESPONSE TEAM. *CERT/Coordination Center Statistics*. 2004. Disponível em: <http://www.cert.org/stats/cert_stats.html>. Acesso em: 09 jan. 2006.

FLORES, F. et al. Computer systems and the design of organizational interaction. *ACM Transactions on Office Information Systems*, v. 6, n. 2, p. 153–172, 1988. Disponível em: <http://doi.acm.org/10.1145/45941.45943>. Acesso em: 07 abr. 2004.

GEER, D.; HOO, K. S.; JAQUITH, A. Information security: why the future belongs to the quants. *IEEE Security & Privacy*, v. 1, n. 4, p. 24–32, July/Aug. 2003.

GLASGOW, J.; MACEWEN, G.; PANANGADEN, P. A logic for reasoning about security. *ACM Transactions on Computer Systems*, v. 10, n. 3, p. 226–264, 1992.

HAGUETE, T. M. F. A interação simbólica. In: _____. *Metodologias qualitativas na sociologia*. 4. ed. Petrópolis: Vozes, 1995. p. 25–50.

HITCHINGS, J. Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security*, v. 14, n. 5, p. 377–383, May 1995.

HUSSERL, E. *Investigações lógicas*: sexta investigação - elementos de uma elucidação fenomenológica do conhecimento. São Paulo: Nova Cultural, 1996.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. *Information security governance*: guidance for boards of directors and executive management. Illinois: Rolling Meadows, 2001.

KIM, J. Phenomenology of digital-being. *Human Studies*, v. 24, n. 1/2, p. 87–111, Mar. 2001.

LIMA, G. A. B. Interfaces entre a ciência da informação e a ciência cognitiva. *Ciência da Informação*, v. 32, n. 1, jan./abr. 2003. Disponível em: <http://www.ibict.br/cionline/320103/3210308.pdf>. Acesso em: 16 ago. 2003.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO - OCDE. *Guidelines for the security of information systems and networks*: towards a culture of security. Paris, 2002. Disponível em: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>. Acesso em: 20 nov. 2002.

PASQUALI, L. *Os tipos humanos*: a teoria da personalidade. Petrópolis: Vozes, 2003.

PEMBLE, M. What do we mean by "information security". *Computer fraud & security*, v. 2004, n. 5, p. 17–19, May 2004.

PRESSMAN, R. S. *Software Engineering*: A practitioner's approach. 2nd. ed. New York: McGraw-Hill, 1995.

SARACEVIC, T. Information science. *Journal of the American Society for Information Science*, v. 50, n. 12, p. 1051–1063, Oct. 1999.

SCHNEIER, B. *Secrets and lies*: digital security in a networked world. New York: John Wiley & Sons, 2000.

STERGIOU, T.; LEESON, M.; GREEN, R. An alternative architectural framework to the OSI security model. *Computers & Security*, v. 23, n. 2, p. 137–153, Mar. 2004.

TAKAHASHI, T. *Sociedade da informação no Brasil*: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TAYLOR, C. To follow a rule... In: CALHOUN, C.; LIPUMA, E.; POSTONE, M. (Ed.). *Bourdieu*: critical perspectives. Chicago: Chicago University, 1993. p. 150–165.

THROOP, C. J.; MURPHY, K. M. Bourdieu and phenomenology: a critical assessment. *Anthropological theory*, v. 2, n. 2, p. 185–207, June 2001.

VENTER, H. S.; ELOFF, J. H. P. A taxonomy for information security technologies. *Computers & Security*, v. 22, n. 4, p. 299–307, May 2003.

VON BERTALANFFY, L. *Teoria Geral dos Sistemas*. Petrópolis: Vozes, 1975.

WOOD, C. C. An unnapreciated reason why information security policies fail. *Computer Fraud & Security*, v. 2000, n. 10, p. 13–14, Oct. 2000.