COMPUTAÇÃO OU ADMINISTRAÇÃO? UMA ANÁLISE SOBRE O PERFIL ADEQUADO PARA O GESTOR DAS POLÍTICAS DE SEGURANÇA

Américo Nobre G. F. Amorim
americoamorim@gmail.com

Jairo S. Dornelas
jairo@ufpe.br

Universidade Federal de Pernambuco, PROPAD, NEPSI – Recife, PE, Brasil

RESUMO

A universalização no uso da tecnologia de informação pelas empresas, ocorrida durante a década de 1990, provocou uma série de mudanças organizacionais. Gerando uma dependência operacional e tática, os principais processos de negócio não podem ser executados a contento quando ocorre uma falha nos sistemas de informação. A segurança é um dos principais aspectos para garantir a confiabilidade dos sistemas de informação. As políticas de segurança estipulam como cada recurso será utilizado e quais os níveis de acesso de cada membro da organização assim como de seus stakeholders. Estas características expressam decisões que estão intimamente relacionadas com aspectos particulares da gestão: a estrutura organizacional, seus processos e sua estratégia de negócio. Neste contexto, é importante tentar identificar qual o perfil adequado do profissional responsável pela gestão da segurança da informação. A identificação de competências e da formação mais adequada para o seu desenvolvimento são temas essenciais para gestores e pesquisadores da área de sistemas de informação. É nesta linha que este ensaio se desenrola, analisando as várias abordagens descritas pela literatura para a elaboração das políticas de segurança. As principais atividades deste profissional são classificadas em três dimensões: técnica, gerencial e estratégica. As conclusões apontam para a necessidade dos profissionais possuírem uma forte interdisciplinaridade, garantindo que o administrador compreende noções básicas das tecnologias que podem influenciar a sua política de segurança e que o profissional de computação tenha conhecimento das diretrizes estratégicas e de sua importância na definição das ações pontuais de segurança.

Palavras-Chave: Política de segurança. Segurança da informação. Profissional de tecnologia. Perfil do Administrador

1. INTRODUÇÃO

A segurança é um dos temas que mais tem merecido atenção dos profissionais que atuam na área de sistemas de informação. Durante a década de 1990, ocorreu uma profunda expansão do uso de computadores e sistemas para os vários departamentos organizacionais. A tecnologia passou a permear todas as funções da empresa como o planejamento do produto, produção, marketing, recursos humanos, contabilidade, finanças e vendas.

Esta profusão tecnológica gerou uma série de efeitos no funcionamento das empresas. Provocando desde pequenas melhorias até o desenho de novos processos, a informatização muda a forma de realizar o trabalho. Cientes dos benefícios advindos do uso de tecnologia, é razoável afirmar que as organizações têm ampliado o ritmo de adoção e a intensidade de uso dos sistemas.

Alguns problemas têm sido causados às organizações pela onipresença dos sistemas de informação baseados em computador (SIBC). O uso freqüente tem levado a uma dependência dessas tecnologias. Grande parte das organizações simplesmente não consegue mais operar com eficiência quando os seus SIBCs estão desativados. Esta constatação ressalta a importância de que existam níveis mínimos de serviço que garantam a operação organizacional.

Vários problemas podem afetar a disponibilidade dos sistemas de informações, destacando-se (STAIR e REYNOLDS, 2002): falhas em componentes físicos (*hardware*), indisponibilidade dos canais de comunicação das redes (*links*), demanda superior à capacidade de atendimento dos servidores, erros de programação e projeto (*bugs*), uso indevido por usuários não autorizados (*hackers*, *crackers)*, vírus e outras pragas eletrônicas.

Nas organizações, a expansão das redes e suas conexões com a Internet têm ampliado os riscos de ação das pragas digitais (vírus, cavalos-de-troia, *spywares* etc) e invasões de sistemas por *hackers*. Estes incidentes podem causar uma série de prejuízos organizacionais, desde a perda, roubo ou alteração ilegal de informações até a indisponibilidade dos serviços de rede, bancos de dados e outros componentes dos sistemas empresariais.

Para lidar com este tipo de ameaça, as organizações se deparam com a necessidade de criar regras que disciplinem o uso da tecnologia de informação e de implementar mecanismos que proporcionem um maior controle desta infra-estrutura essencial. É neste contexto em que ocorrem as definições para as políticas e práticas de segurança em sistemas de informação.

As políticas de segurança visam estipular como cada recurso será utilizado e quais os níveis de acesso de cada membro da organização e também de seus *stakeholders*. Estas características expressam decisões que estão intimamente relacionadas com aspectos particulares da gestão: a estrutura organizacional, seus processos e sua estratégia de negócio.

Assim, é razoável afirmar que a política de segurança é um artefato cuja gênese deve ocorrer no seio da gestão empresarial. Seria natural imaginar que a definição das políticas de segurança fosse tarefa desempenhada por profissionais com formação em gestão organizacional. Curiosamente, verifica-se que na prática empresarial ocorre o oposto, profissionais sem formação em gestão são encarregados por criar e manter as políticas de segurança.

Assim, é importante tentar identificar qual seria o perfil adequado do profissional responsável pela gestão segurança da informação. A identificação de competências e da formação mais adequada para o seu desenvolvimento é um tema essencial para gestores e pesquisadores da área de sistemas de informação.

É nesta linha que este ensaio se desenrola, analisando a elaboração das políticas de segurança, buscam-se elementos que possam indicar um perfil adequado para o gestor das políticas de segurança. Este trabalho pretende fornecer elementos para reflexão acerca desta questão.

2. SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

A segurança de sistemas de informação computadorizados representa um conjunto de práticas e ações que são empreendidas para que sejam atingidos os seguintes objetivos básicos de segurança (ESCAMILLA, 1998):

- Confidencialidade, proteção das informações sensíveis para que não sejam disponibilizadas aos usuários não-autorizados;
- Integridade para manter os dados a salvo de modificações não autorizadas, garantindo a sua confiabilidade e veracidade;
- Acessibilidade para permitir que usuários autorizados possam utilizar os recursos a que tem direito e negar acesso aos usuários indesejados.

Para atingir estes objetivos, o administrador de sistemas deve estar ciente de que nenhuma rede ou sistema é completamente seguro (SMITH *et al*, 2004). Ou seja, quanto mais importante for um ativo, mais exposto aos incidentes de segurança ele estará. Entendendo os riscos inerentes aos sistemas, os gestores devem buscar formas para gerenciar as ameaças.

O gerenciamento de riscos envolve uma série de atividades que vão desde o levantamento dos recursos e seus valores, previsão de possíveis ataques até a monitoração dos ativos. Para cada conjunto de riscos identificados, o gestor deve decidir entre qual curso de ação irá empreender (DORFMAN, 1997):

- Aceitar a ameaça, não tomando nenhuma atitude sobre o risco. Esta forma é indicada quando os custos de mitigação do risco são percebidos como elevados, não sendo viáveis. Nestes casos apenas um plano de contingência é elaborado, indicando quais ações serão tomadas caso o risco se manifeste.
- Mitigar o risco através da implementação de ações que reduzam a exposição do recurso às ameaças. Outra abordagem se dá quando a organização implementa medidas que reduzem a importância do ativo em risco. Em ambos os casos o administrador deve estar atento para os riscos envolvidos no processo e nos benefícios obtidos.
- Transferir o risco para um parceiro especializado. Ao delegar o gerenciamento de um risco ao parceiro, a organização ganha economias de especialização e escala. Nesta modalidade estão desde as apólices de seguro até os serviços de hospedagem de sites.
- Evitar o risco através da remoção do recurso, da ameaça ou da dependência da organização sobre o ativo. Quando as demais estratégias não forem indicadas ou viáveis. Se a análise indica que é melhor não ter o ativo do que enfrentar os riscos, a organização deverá se desfazer dele.

3. INCIDENTES DE SEGURANÇA

Os incidentes envolvendo segurança de sistemas ocupam parte significativa dos recursos de tecnologia da informação das organizações. Apenas no Brasil, em 2005, foram registrados mais de 68 mil incidentes de segurança em redes conectadas à internet (CERT, 2006). Estes casos incluem ataques contra computadores pessoais, tentativas de obtenção de informações empresariais, difusão de vírus e cavalos-de-troia e ataques para congestionar ou desativar redes de empresas e provedores de acesso.

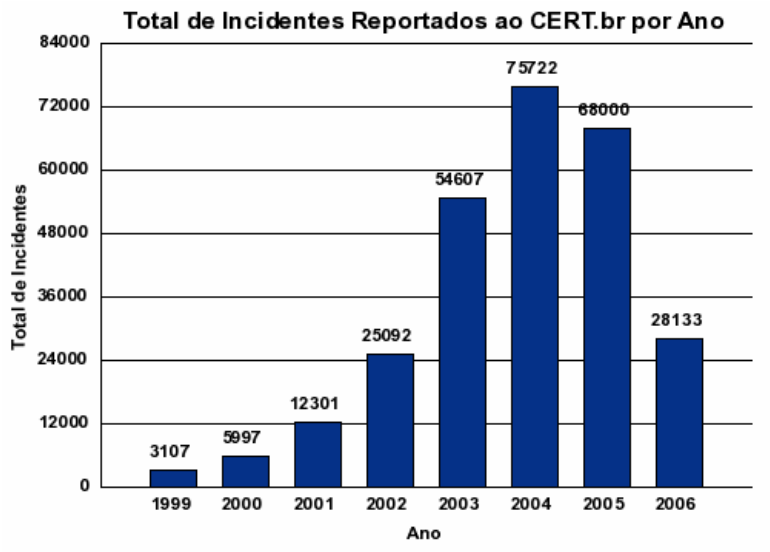

Figura 01. Evolução dos Incidentes De Segurança

Fonte: CERT (2006)

Os incidentes de segurança são ocasionados por falhas de diversas naturezas como (SONNENREICH e ALBANESE, 2004):

- Erros humanos que ampliam as vulnerabilidades dos sistemas. Os erros podem compreender uma série de situações como o uso de senhas fáceis de descobrir e ataques de engenharia social. Neste último caso, a pessoa é enganada e levada a passar alguma informação ou executar um procedimento para um usuário não autorizado;
- Erros na política de segurança ou simplesmente sua inexistência. As políticas de segurança falham principalmente: quando são vagas, não especificando procedimentos e responsáveis; quando estão desatualizadas e principalmente quando não existem mecanismos de controle e monitoramento dos recursos;
- Erros de configuração de equipamentos como servidores e *firewalls;*
- Ignorância dos gestores sobre os riscos e aspectos processuais e tecnológicos;
- Falta de atualização nas políticas, ferramentas e mecanismos de segurança, tornando-os obsoletos.

Para verificar a segurança dos sistemas as organizações podem utilizar uma série de técnicas como as varreduras para buscar vulnerabilidades em sistemas, servidores e estações de trabalho, testes de penetração para verificar a eficácia dos mecanismos de isolamento e segurança e por fim as auditorias de segurança (SMITH *et al*, 2004).

Com a expansão da tecnologia de informação para todos os níveis das organizacionais, e o surgimento de organizações virtuais, que tem sua existência viabilizada pela tecnologia, os incidentes de segurança tornam-se ameaças reais à operação e estratégia empresarial. De sorte que, quanto maior for a adoção tecnológica, maior a necessidade de estabelecer mecanismos de proteção contra invasões e pragas digitais. Uma das formas tradicionalmente relatadas é a utilização de políticas de segurança.

4. POLÍTICAS DE SEGURANÇAS

As políticas de segurança têm sido estudadas por duas óticas divergentes. O primeiro grupo utiliza o termo "política de segurança" para descrever regras de controle e acesso aos sistemas (SANDHU e SAMARATI, 1994). Nesta linha, a política de segurança "não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas" que utilizam os sistemas (CERT, 2003).

O segundo grupo atua com um olhar organizacional. Tanenbaum (1992) entende que a política indica os recursos que serão protegidos e os mecanismos de segurança definem como a política será praticada e garantida. Abrams e Bailey (1995) classificam as políticas em três dimensões:

- Política de segurança corporativa, elaborada de acordo com a visão da alta gestão;
- Política de segurança organizacional, elaborada de acordo com a visão dos usuários dos sistemas de informação;
- Política de segurança técnica, elaborada para atender aos requisitos dos responsáveis pela implementação e pelos sistemas de controle.

Wood (1999) define "política" como declarações contendo linhas gerais que a alta administração determina e que devem ser seguidas obrigatoriamente por todos os membros. Baskerville e Siponen (2002) adotam uma terminologia baseada em três níveis:

- Um plano da alta gestão que aborda os objetivos relacionados com a segurança e os procedimentos aceitáveis para a operação;
- Um plano gerencial com que reflete de forma menos abstrata o plano da alta gestão. Neste nível os processos organizacionais são referenciados, identificando como se dá

seu acoplamento com as práticas de segurança. Também são definidas medidas de combate às ameaças (*firewalls*, anti-virus etc) e sanções para descumprimentos da política;

- Uma meta-política que indica como a organização cria e mantêm a sua política de segurança. Entre suas atribuições, definirá quem são os responsáveis pela elaboração e modificação das políticas de segurança e em quais momentos este processo deve ser iniciado.

Solms (1999) identifica duas perspectivas, a segurança técnica que busca os mecanismos tecnológicos para assegurar a integridade dos sistemas e a perspectiva operacional. Na dimensão operacional, Solms (1999) inclui atividades como um fórum de segurança composto por profissionais de vários setores para elaboração das políticas de segurança e também a figura do *Chief Security Officer*, executivo encarregado dos aspectos de segurança em toda a organização.

Smith *et al* (2004) define três dimensões para a política de segurança:

- Políticas administrativas que são exercidas através de processos gerenciais para suprir aspectos que não são abordados por *software*, *hardware* e os demais componentes dos sistemas. Um exemplo deste tipo de política são os termos de sigilo que garantem que os *stakeholders* não irão repassar informações sensíveis a terceiros;
- Políticas técnicas que são exercidas pelos sistemas operacionais, aplicativos e outros meios de controle técnicos. Mecanismos que garantem um mínimo de complexidade as senhas utilizadas pelos usuários estão nesta dimensão;
- Políticas físicas que previnem intervenções e roubos aos recursos de *hardware* da organização. O isolamento de servidores em ambientes controlados por rígidos mecanismos de segurança (alarmes, acesso por leitura biométrica) é um exemplo desta dimensão.

Autor	Aspectos Estratégicos	Aspectos Gerenciais	Aspectos Técnicos
Sandhu e Samarati (1994)			
CERT (2003)			
Tanenbaum (1992)			
Abrams e Bailey (1995)			
Solms (1999)			
Baskerville e Siponen (2002)			
Smith *et al* (2004)			

Quadro 1. Síntese das Dimensões de Política de Segurança.

A utilização de padrões e modelos para formulação e avaliação das políticas de segurança tem sido apontada como uma boa prática (CHOKHANI, 1992; CAPLAN E SANDERS, 1999). No pólo oposto, Dhillon (1997) defende que ao invés de determinar políticas, as organizações devem elaborar uma visão e uma estratégia sobre a segurança nos níveis de alta gestão, definindo um processo de modelagem de responsabilidades.

Estas concepções reforçam a importância da dimensão técnica das políticas de segurança. Também fica evidente a importância da atuação dos níveis gerencial e estratégico. Isto decorre do fato de que, com a disseminação da tecnologia de informação, quase todas as funções organizacionais são afetadas por políticas que regulem a forma de uso da tecnologia.

As práticas administrativas citadas por Smith (1994) deixam clara a importância de controles fundamentados em processos em gestão, o que não pode ser efetuado na plenitude por profissionais sem competências administrativas. Os planos da alta gestão definidos por

Baskerville e Siponen (2002) e a visão de segurança de Abrams e Bailey (1995) exigem dos formuladores conhecimentos de gestão estratégica.

No nível estratégico, a política de segurança deve ser perfeitamente acoplada aos objetivos e a visão do negócio para que sua execução não traga prejuízos a implantação das estratégias. Isto se reflete em vários aspectos do negócio, desde as operações até a forma de se relacionar com clientes, fornecedores e parceiros.

Empresas que tem uma estratégia orientada pela transparência e compartilhamento de informações com *stakeholders* precisam ter políticas de segurança que abordem estes requisitos, fornecendo meios para viabilizar a estratégia. Estas características reforçam a importância de conhecimentos e experiência gerencial nos formuladores da política de segurança.

5. PROBLEMAS DAS POLÍTICAS DE SEGURANÇA

Baskerville e Siponen (2002) indicam que os estudos sobre políticas de segurança têm focado principalmente problemas como os conteúdos que devem estar presentes nas políticas (ANDERSON, 1996; KWOK e LONGLEY, 1997) e as dificuldades relacionadas com a conquista de apoio da alta gestão para as políticas (PERRY, 1985; KWOK e LONGLEY, 1997).

A segunda característica é bastante relevante. O problema reportado pelos formuladores de políticas de segurança, que a alta gestão não apóia as determinações, revela uma séria questão organizacional. Se as políticas de segurança devem ser definidas nos níveis estratégicos e gerenciais, é esperado que exista comprometimento da alta-gestão para a sua implementação. As dificuldades em obter comprometimento indicam que, na prática empresarial, as políticas podem não estar sendo definidas nos níveis gerencial e estratégico.

Outra possibilidade é que estejam sendo idealizadas e propostas por profissionais da área de computação. Devido a sua formação técnica, é provável que estas políticas não contemplem as necessidades das diversas funções organizacionais. Casos extremos nos quais a política é tão técnica que os gestores não a compreendem também podem ocorrer.

Outro problema identificado por Baskerville e Siponen (2002) é que, muitas vezes, o processo de definição das políticas fica preso à aplicação dos modelos e padrões, reduzindo a atenção às tarefas de análise e investigação. Ao utilizar quase que diretamente os padrões, as organizações ignoram questões sociais, suas idiossincrasias, estratégias e requisitos de negócio. Estas negligências podem causar sérios problemas de segurança, desde medidas ineficazes até mecanismos que prejudiquem a condução dos negócios.

Disfunções como estas reforçam a importância dos aspectos organizacionais que devem estar presentes na política de segurança. A aplicação direta de modelos e padrões pode indicar uma característica de profissionais que apenas percebem a dimensão técnica da segurança.

6. CONCLUSÕES

A difusão da tecnologia de informação por todas as áreas funcionais e o surgimento de organizações virtuais amplia a importância das políticas de segurança. Muito mais do que simples procedimentos técnicos que controlam o acesso aos sistemas, é necessário que a política de segurança suporte a operação e os rumos da estratégia de negócio.

Diante destes requisitos, pensar em um profissional que esteja apto a conduzir a elaboração e manutenção de uma política de segurança implica necessariamente em considerar competências gerenciais e estratégicas.

Assim, a defesa de um perfil técnico com formação em computação para desempenhar uma função que requer habilidades clássicas do administrador é uma visão ingênua. Os que partilham desta concepção desconhecem a importância contemporânea da segurança e sua influencia sobre a performance organizacional.

É razoável afirmar que a política de segurança deve ser encarada sob duas óticas: o prisma organizacional, abordando as questões estratégicas e operacionais, e sob o prima tecnológico, que busca a melhor forma de implementar as decisões organizacionais. Para cumprir estas duas funções, a organização poderá designar dois profissionais, um com formação em gestão e outro em computação.

Mesmo neste nível de especialização, estes profissionais devem possuir uma forte interdisciplinaridade, garantindo que o administrador compreende noções básicas das tecnologias que podem influenciar a sua política de segurança e que o profissional de computação tenha conhecimento das diretrizes estratégicas e de sua importância na definição das ações pontuais de segurança.

Aceitando-se a definição destes dois eixos de atuação, o fato de que frequentemente as políticas de segurança são definidas por profissionais sem formação em gestão pode indicar uma timidez dos administradores. Quiçá, por não compreenderem que a segurança é uma função pelo menos tão organizacional quanto tecnológica, eles não vejam importância em gerenciá-la, delegando para os profissionais de informática.

Outra conseqüência da visão míope sobre a segurança é a aparente aversão de administradores às questões tecnológicas. Como não percebem como importante, não buscam estudar e compreender os aspectos básicos da tecnologia que influi na segurança de suas empresas.

Estes comportamentos são perigosos, podendo gerar prejuízos sérios para a organização. Cientes da necessidade de ter administradores também envolvidos nas questões de segurança, a alta-gestão pode, e deve, tomar medidas para incluir no perfil de seus gestores uma formação básica que ressalte as tecnologias de segurança e a importância de suas interfaces com as diretrizes gerenciais e estratégicas.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMS, M.D.; BAILEY, D. Abstraction and refinement of layered security policy, in ABRAMS, M.D, JAJODIA, S., PODELL, H.J. , Information Security – An integrated Collection of Essays, IEEE Computer Society Press, 1995.

ALBANESE, Jason; SONNENREICH, Wes. Network Security Illustrated. McGraw-Hill, 2004.

ANDERSON, R. A security policy model for clinical information systems, 1996.

BASKERVILLE, Richard; SIPONEN, Mikko. An information security meta-policy for emergent organizations. Logistics Information Management, v. 15, n. 5/6, p. 337-346, 2002.

CAPLAN, K.; SANDERS, J.L. Building an international security standard, IEEE IT Professional, v. 1, n. 2, p. 29-34, 1999.

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Práticas de Segurança para Administradores de Redes Internet, 2003. Disponível em: <http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-redes.pdf> Acesso: 13-07-06.

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Estatísticas dos Incidentes Reportados ao CERT.br, 2006. Disponível em: <http://www.cert.br> Acesso: 13-07-06.

CHOKHANI, S. Trusted products evaluation, Communications of the ACM, v. 35, n. 7, p.64-76, 1992.

DHILLON, G. Managing Information Systems Security, Macmillan Press, 1997.

DORFMAN, Mark S. Introduction to Risk Management and Insurance. Prentice Hall, 1997.

ESCAMILLA, Terry. Intrusion Detection: Network Security beyond the Firewall. John Wiley & Sons, 1998.

PERRY, W.E. Management Strategies for Computer Security, Butterworth-Heinemann, 1985.

SANDHU, R.S.; SAMARATI, P. Access control: principles and practice, IEEE Communications, p. 40-48, 1994.

SMITH, Ben; LEBLANCK, David; LAM, Kevin. Assessing Network Security. Microsoft Press, 2004.

SOLMS, Rossouw von. Information security management: why standards are important. Information Management & Computer Security, n.7, v.1, p. 50-57, 1999.

STAIR, Ralph; REYNOLDS, George W. Princípios de Sistemas de Informação. Rio de Janeiro: LTC, 2002.

TANENBAUM, A. Modern Operating Systems, Prentice-Hall, 1992.

WOK, L. LONGLEY, D. Code of practice: a standard for information security management, Proceedings of the IFIP TC11 13th International Conference on Information Security, SEC'97, Copenhagen, 1997.

WOOD, C.C. Information Security Policies Made Easy, Baseline *Software*, 1999.