Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799[1]

Autoria: Rodrigo Polydoro Oliva, Mírian Oliveira

Resumo

A tecnologia da informação e a Internet tornaram-se uma plataforma vital de transações entre as empresas e seus funcionários, clientes, fornecedores e parceiros comerciais. No entanto, todos os benefícios trazidos pela utilização de sistemas de informação podem não ser alcançado devido a problemas de segurança da informação. O objetivo desta pesquisa é analisar a percepção dos diretores de tecnologia, gerentes de tecnologia ou *security officers* sobre o processo de elaboração, implantação e manutenção da política de segurança comparando com as recomendações da NBR/ISO17799. O método adotado foi a survey. O instrumento foi enviado via web para diretores de tecnologia, gerentes de tecnologia ou *security officers* de 194 empresas localizadas no Rio Grande do Sul, selecionadas por conveniência. A taxa de resposta foi 27,31% (53 respondentes). Como principais resultados pode-se citar: que as empresas percebem que um incidente de segurança pode causar impacto na competitividade da organização no mercado; a maioria das empresas que já possuem a política de segurança não utilizou a NBR/ISO17799, no entanto, seguiram as boas práticas no processo de elaboração, realizando uma Análise de Risco.

1 Introdução

Hoje, pode-se dizer que a tecnologia da informação e a Internet tornaram-se uma plataforma vital de transações entre as empresas e seus funcionários, clientes, fornecedores e parceiros comerciais. Devido à globalização dos mercados e à concorrência cada vez mais acirrada, as empresas estão revendo seus paradigmas e buscando mecanismos de sobrevivência, a fim de preservar o seu *market share* e a continuidade no negócio. A velocidade, qualidade e eficiência das comunicações são as principais características na busca pela competitividade nesta nova visão de mercado (NAKAMURA e GEUS, 2002). Para que isso ocorra, as organizações precisam elaborar estratégias competitivas sustentáveis que busquem aumentar a sua rentabilidade e, assim, conseguir vantagem competitiva.

Na busca pela competitividade, lucratividade e para suportar as estratégias competitivas as organizações estão utilizando diversas tecnologias, entre elas os sistemas de informação (O'BRIEN, 2001; PORTER, 1989). No entanto, todos os benefícios trazidos pela utilização de sistemas de informação podem não ser alcançado devido a problemas de segurança da informação. De acordo com pesquisa realizada pelo *Computer Security Institute* - CSI e *Federal Bureau of Investigation's - FBI*, as principais quebras de segurança nos sistemas de informação ocorrem por: vandalismo, espionagem industrial, descontentamento de funcionários internos, concorrência desleal (POWER, 2002). As perdas financeiras referentes a problemas com segurança da informação nos Estados Unidos em 2001, foram de US$ 455.848.000 e o total registrado entre 1997 e 2001 foi de US$ 1.459.755.245 (POWER, 2002). Com esses motivos e com o lançamento da ISO/IEC 17799, Código de Prática para a Gestão da Segurança da Informação, que apresenta as melhores práticas para essa gestão, as empresas aumentaram os seus investimentos em segurança da informação, entre eles o desenvolvimento de políticas de segurança.

O desenvolvimento da política de segurança é o principal e o primeiro passo da estratégia de segurança (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001). Ela considera todos os aspectos relativos à criação, manipulação e eventual destruição da informação, esteja ela em meio eletrônico, papel ou outra mídia. Desta forma, o objetivo desta pesquisa é analisar a percepção dos diretores de tecnologia, gerentes de tecnologia ou *security officers* sobre o processo de elaboração, implantação e manutenção da política de segurança comparando com as recomendações da NBR/ISO17799.

A seção 2 apresenta a gestão da segurança da informação e a NBR/ISO17799, e a seção 3 trata do processo de elaboração, implantação e manutenção da política de segurança. Na seqüência, na seção 4, o método utilizado para o desenvolvimento desta pesquisa é descrito. Na seção 5, são discutidos os resultados obtidos na pesquisa de campo. Por último, as conclusões são colocadas na seção 6.

2 Gestão de Segurança da Informação e a NBR/ISO17799

A gestão de um negócio e a tomada de decisão são baseadas em informações que a organização possui. Este processo envolve riscos e a gerência deles é imprescindível para a empresa (NAVARRO, 2001). Tudo isso ocorre, uma vez que as informações compõem, segundo Freitas e Lesca (1992), um recurso estratégico para o sucesso da empresa junto a sua concorrência. Por isso, a informação é um ativo da organização tão importante quanto qualquer outro e deve ser protegido devido ao seu valor (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; YAPP, 2000).

Com o grande uso de redes de computadores, sistemas de telecomunicações e a Internet, as organizações estão expostas a riscos antes desconhecidos (NAVARRO, 2001; DIPPEL, 2000). Balarine (2002) salienta, por exemplo, que um dos fatores que limita o crescimento do comércio eletrônico são os problemas de segurança.

Devido a este ambiente inseguro, as empresas necessitam de um processo de gestão da segurança da informação, cujo objetivo é proteger os interesses da organização e ter confiança nas informações, nos sistemas e nas comunicações onde elas trafegam (WILLIAMS, 2001). Desta forma, grandes empresas, agências governamentais e instituições internacionais têm trabalhado para estabelecer padrões e normas que reflitam as melhores práticas de mercado relacionadas à segurança dos sistemas e informações (DHILLON e BACKHOUSE, 2001; MASON, 2000).

Em 1989 o *Commercial Computer Security Center*, órgão ligado ao departamento de indústria e comércio do Reino Unido, publicou a primeira versão do PD0003 – Código para Gerenciamento de Segurança da Informação (ROCHA, 2002). Em 1995 este código foi revisado e publicado como um *British Standard*, com a denominação de BS 7799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e crescimento da segurança da informação (BASTOS, 2002). A BS 7799 foi revisada e atualizada em 1999 com o acréscimo de novos controles devido às novas necessidades de mercado como o comércio eletrônico, computação móvel entre outros aspectos, sendo publicada como Parte 1, BS 7799-1:1999 (BSI, 2002). Devido ao interesse internacional em uma norma de segurança da informação a BS 7799-1:1999 foi submetida à ISO pelo método de *fast track*. Assim, em dezembro de 2000 a Parte 1 BS 7799-1:1999 foi publicada como norma internacional ISO/IEC 17799:2000, após aprovação em outubro na reunião do Comitê Internacional de Normatização realizada em Tóquio, Japão. Em 2001, a Associação Brasileira de Normas Técnicas (ABNT), publicou a versão brasileira da ISO/IEC 17799:2000 que ficou com a denominação de NBR/ISO17799 – Código de Prática para a Gestão da Segurança da Informação (NAKAMURA E GEUS, 2002).

A Parte 2 foi publicada como BS 7799-2:1998, que especifica os controles de segurança que devem ser implementados de acordo com necessidades do negócio e das requisições legais para a obtenção da certificação de segurança nesta norma. Hoje se uma empresa brasileira desejar obter uma certificação em segurança da informação, ela deve se adequar às práticas determinadas na NBR/ISO 17799 e ser auditada conforme os padrões estabelecido na BS 7799-2:2002 (BRITISH STANDARD, 2002). Já existem no mundo 194 empresas certificadas, das quais 192 em países como Reino Unido (82), Japão (21), Coréia (9), Índia (9), Alemanha (8), Finlândia (8). No Brasil existem duas empresas certificadas SERASA-SP e Módulo (REGISTER INTERNATIONAL, 2002).

A norma NBR/ISO 17799 define 127 controles que podem compor o escopo do sistema de gerência de segurança (*Information Security Management System* - ISMS), enfocando o processo sob o ponto de vista do negócio da empresa (TREGEAR, 2001). A norma trata de aspectos como política de segurança, segurança organizacional, classificação e controles dos ativos da informação, segurança em pessoas, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acesso, desenvolvimento e manutenção de sistemas, gestão da continuidade do negócio e conformidade.

Os pilares que sustentam a segurança da informação são: confidencialidade, integridade e disponibilidade (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; WILLIAMS, 2001; MASON, 2000). A confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; BONCELLA, 2002). A integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas não possam modificá-la, adicioná-la ou removê-la (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; FISCH e WHITE, 2000 apud URCUYO e KUNNATHUR, 2002; BONCELLA, 2002). Já a disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; URCUYO e KUNNATHUR, 2002; BONCELLA, 2002).

Esses pilares balizadores são constantemente ameaçados de diversas formas como incêndio, falha de energia elétrica, mau funcionamento do hardware, erros de software, erros de usuários, crime por computador e mau uso do computador (LAUDON e LAUDON, 1999). A ameaça principal é o crime por computador (DIPPEL, 2000; LAUDON e LAUDON, 1999), que pode variar de uma brincadeira de adolescente à espionagem industrial. Devido à concentração das informações em uma organização, o crime por computador torna-se um aspecto de elevadas perdas e alto risco para uma empresa comercial (LAUDON e LAUDON, 2000). Townsend (apud RASHBAUM, 2002) confirma isso: "*nós vivemos em um mundo onde o teclado do computador tem um potencial enorme de causar prejuízos*". No cenário brasileiro percebe-se o mesmo perfil, de acordo com a 8ª Pesquisa Nacional de Segurança da Informação (MODULO, 2002), 55% dos entrevistados consideravam a Internet com o principal ponto de ataque aos seus sistemas de informação e os *hackers* foram os maiores responsáveis pelos ataques e invasões de 2002, tendo um percentual de 48%.

De acordo com a pesquisa *Global Information Security Survey* (KPMG, 2002), os incidentes de vírus paralisam as empresas americanas, em média, por 68 dias/ano e quantificam uma perda média de US$ 162,000 por ano. Além disso, as perdas de informações confidencia□□is geraram uma perda média de US$ 197 mil. Já no Brasil, 78% das empresas entrevistadas (MODULO, 2002) tiveram perdas financeiras decorrentes de ataques e invasões de seus sistemas de informação. Contudopenas 45% das empresas conseguem quantificar estas perdas e que tem a seguinte participação: 12% com perdas de até R$ 50 mil no ano, 7% com perdas entre R$ 50 mil e R$ 500 mil, 2% com perdas entre R$ 500 mil e R$ 1 milhão e apenas 1% com perdas superiores à R$ 1 milhão.

Em muitos casos, essas perdas podem ser diminuídas com a adoção de um processo de gestão de segurança, onde está incluída a Política de Segurança (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; WILLIAMS, 2001).

3 Política de Segurança

Os ativos da informação são críticos para as organizações, já que muitas das tecnologias e conhecimentos são empregados no desenvolvimento do negócio (YAPP, 2000). Desta forma, é importante entender a necessidade da segurança da informação, expressa através de normas e guias que formam a política de segurança (CAVUSOGLU, MISHRA e RAGHUNATHAN, 2002; WILLIAMS, 2001).

Um dos fatores críticos para o sucesso da implementação da cultura de segurança da informação dentro de uma organização é a política de segurança, considerada uma das melhores práticas para a segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; WILLIAMS, 2001). A política de segurança é a base para todas as questões relacionadas à empresa. Ela é o primeiro passo e um dos principais para a elaboração da estratégia de segurança na organização (NAKAMURA e GEUS, 2002).

Dentro da visão do planejamento de segurança, a política de segurança é o topo, logo acima das normas e procedimentos (NAKAMURA e GEUS, 2002; PATRICK, 2002). Segundo a empresa *e-trust* especializada em segurança da informação (E-TRUST, 2002), a política de segurança é o nome genérico para regras, que em vários níveis estabelecem o comportamento e as ferramentas disponíveis ou necessárias para manter o nível de segurança adequado à organização. As regras de uma política de segurança são instruções, necessariamente aprovadas pela alta direção da empresa, que indicam um curso de ação, um princípio guiando, ou um procedimento que seja apropriado, prudente, ou vantajoso. Este conceito é reforçado pela NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001) que apresenta como objetivo de uma política de segurança, o provimento à direção da organização de uma orientação e apoio à segurança da informação.

A NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001), apresenta as recomendações para o processo de elaboração, implantação e manutenção da política de segurança. Para a elaboração da política de segurança é necessário que a organização realize, primeiramente, uma análise de risco para identificar as ameaças aos ativos da informação, as vulnerabilidades nos sistemas e avaliar a probabilidade de ocorrência e o impacto que teria no negócio (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001; TREGEAR, 2001; DHILLON e BACKHOUSE, 2001). A realização desta avaliação de risco permitirá à organização identificar os seus pontos críticos e assim desenvolver uma política de segurança que proteja em um maior nível os ativos que possam causar maior prejuízo ao negócio (E-TRUST, 2002).

Após a realização da análise de risco parte-se para a elaboração do documento da política de segurança que deve considerar, no mínimo, as seguintes orientações de acordo com a NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001): a) apresentação da definição de segurança da informação, o escopo que ela contempla, as metas e a importância da segurança como um mecanismo que habilita o compartilhamento da informação; b) declaração de comprometimento da alta direção apoiando as metas e os princípios da segurança da informação; c) explanação das políticas específicas, princípios, padrões e requisitos de conformidade de importância específica para a organização de acordo com a avaliação de risco; d) definição das responsabilidades gerais e específicas na gestão de segurança da informação, incluindo os registros de segurança; e) referência a documentos que possam apoiar a política de segurança, como procedimentos de segurança e regras para usuário.

Além dessas orientações a NBR/ISO17799 recomenda uma estrutura para a elaboração das políticas específicas que deve contemplar os seguinte itens: política de segurança organizacional, política de classificação e controle de ativos da informação, política de segurança em pessoas, política de segurança física e do ambiente, política de gerenciamento das operações e comunicações, política de controle de acesso, política de desenvolvimento e manutenção de sistemas, política de gestão de continuidade no negócio, política de conformidade.

Realizado o processo de elaboração da política de segurança é necessário que a mesma seja implantada e tenha uma manutenção periódica, a fim de se adequar às necessidades de segurança exigidas pelo negócio da empresa. Para o processo de implantação da política de segurança, segundo a NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS

TÉCNICAS, 2001), é necessário que a mesma seja divulgada para todos os colaboradores da organização de forma relevante. Além disso, a política de segurança deve estar acessível e compreensível para todos.

A manutenção da política de segurança, de acordo com a NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001), passa primeiramente pela definição de um gestor que seja responsável pela manutenção e pela análise crítica, que deve ser periódica e contemplar os seguintes itens: efetividade da política de segurança, custo e impacto dos controles na eficiência do negócio e efeitos das mudanças na tecnologia. Desta maneira, percebe-se a dimensão que a política de segurança deve possui em uma organização para que os ativos da informação possam ser protegidos adequadamente de acordo com o seu valor.

4 Método

O método adotado nesta pesquisa foi a survey, em função do objetivo da mesma. O método survey, segundo Malhotra (2001, p. 179), "*se baseia no interrogatório dos participantes da pesquisa, através de perguntas que abordem o comportamento, atitude, intenções, características entre outros aspectos*".

Inicialmente, realizou-se uma revisão na literatura sobre gestão da segurança da informação e política de segurança. Na seqüência, foram realizadas as entrevistas de profundidade (em novembro de 2002), com dois especialistas em segurança da informação com amplo conhecimento dos processos de gestão da segurança da informação, e experiência na condução de projetos deste tipo em grandes empresas brasileiras e internacionais, e com o diretor de uma das maiores empresas do Rio Grande do Sul. Estas entrevistas foram realizadas com o objetivo de coletar informações suplementares para auxiliar na elaboração do instrumento de pesquisa final.

Na fase descritiva foram realizadas as seguintes ações: identificação das empresas a serem pesquisadas, elaboração e validação do instrumento, pré-teste, aplicação do instrumento e análise dos dados.

As 194 empresas foram selecionadas por conveniência, todas localizadas no Rio Grande do Sul, tendo obtido 53 respostas válidas (taxa de retorno de 27,31%). Em paralelo à seleção das empresas a serem pesquisadas, elaborou-se o instrumento de pesquisa. Ele foi realizado de acordo com a Revisão da Literatura e dos resultados da Fase Exploratória. Devido aos diferentes estágios da política de segurança nas organizações, chegou-se a dois tipos de instrumento de pesquisa. Um deles voltado para as empresas que possuem política de segurança, e o outro para as empresas onde a política de segurança está em desenvolvimento ou não possuem. O instrumento é composto de perguntas sócio-demográficas e referentes à política de segurança da informação (importância; processo de elaboração, implantação e manutenção).

Com o instrumento elaborado foi realizada a validação de seu conteúdo por 2 professores doutores. Posteriormente, realizou-se o pré-teste do instrumento com 10 empresas. O instrumento foi aplicado via *web,* em dezembro e janeiro de 2002*,* devido a alguns fatores importantes destacados na avaliação comparativa apresentada por Malhotra (2001). Inicialmente, foi enviada uma mensagem de correio eletrônico para as empresas selecionadas, explicando os objetivos da pesquisa e o endereço do *site*. Como reforço foi enviada uma nova mensagem eletrônica e posteriormente um telefonema.

5 Apresentação, Análise e Discussão dos Resultados

Inicialmente, são apresentados os resultados referentes à caracterização das empresas pesquisadas (5.1). Na seqüência, são abordados os aspectos relativos à importância da política de segurança da informação (5.2), processo de elaboração, implantação e manutenção (5.3).

5.1 Caracterização das Empresas Pesquisadas e dos Respondentes

Do total de respostas válidas (53), a maioria já possuía uma política de segurança (54,72%), ou está no processo de desenvolvimento (26,42%), e apenas 18,87% das empresas ainda não possuem uma política de segurança formalizada.

O perfil das empresas que participaram desta pesquisa está dividido em diversos segmentos, como mostra a tabela 1, sendo que no geral a indústria é a mais representativa com 39,62%, seguida do setor serviços 13,21% e os setores de menor participação são o de informática com 5,66% e o setor governo que não teve nenhuma representatividade. O segmento outros é representado por petroquímico, agropecuária, educação e multimídia.

Percebe-se que todas as empresas do segmento financeiro possuem uma política de segurança ou estão em desenvolvimento. Isto talvez ocorra devido às novas mudanças impostas, pelo Banco Central do Brasil com a entrada do novo Sistema de Pagamentos Brasileiro (SPB).

Tabela 1 - Ramo de Atividade

Ramo de Atividade	Sim	Está em desenvolvimento	Não	Total
Indústria	44,83% (13)	28,57% (4)	40,00% (4)	39,62% (21)
Comércio	3,45% (1)	28,57% (4)	10,00 (1)	11,32% (6)
Segmento Financeiro	17,24% (5)	7,14% (1)	0,00% (0)	11,32% (6)
Serviços	10,34% (3)	21,43% (3)	10,00 (1)	13,21% (7)
Informática	6,90 (2)	0,00% (0)	10,00 (1)	5,66% (3)
Telecomunicações	10,34% (3)	0,00% (0)	30,00% (3)	11,32% (6)
Outros	6,90% (2)	14,29% (2)	0,00% (0)	7,55% (4)
Total	100,00% (29)	100,00% (14)	100,00% (10)	100,00% (53)

Além disso, pode-se observar que as empresas possuem faturamento médio anual entre R$ 50 milhões e mais de R$ 500 milhões, de acordo com a tabela 2. Percebe-se que a maioria das empresas que possuem política de segurança ou estão desenvolvendo-a são as que têm faturamento médio anual superior a R$ 500 milhões. Este resultado pode ser um indicativo de que as empresas de maior porte podem ter uma maior preocupação com a gestão da segurança de suas informações e por isso já possuem uma política de segurança ou já estão desenvolvendo-a.

Tabela 2 - Faturamento

Faturamento	Sim	Está em desenvolvimento	Não	Total
Até R$ 50 milhões	20,69% (6)	14,29% (2)	40,00% (4)	22,64% (12)
De R$ 51 milhões a R$ 100 milhões	10,34% (3)	14,29% (2)	10,00% (1)	11,32% (6)
De R$ 101 milhões a R$ 300 milhões	17,24% (5)	14,29% (2)	10,00% (1)	15,09% (8)
De R$ 301 milhões a R$ 500 milhões	6,90% (2)	14,29% (2)	10,00% (1)	9,43% (5)
Mais de R$ 500 milhões	44,83% (13)	42,86% (6)	30,00% (3)	41,51% (22)
Total	100,00% (29)	100,00% (14)	100,00% (10)	100,00% (53)

O perfil dos respondentes é representado pelos responsáveis pela segurança da informação nas empresas e é composto de uma pequena parcela de diretores de tecnologia (5,66%), por gerentes de tecnologia (50,94%) e *security officer* (32,08%). Este último é um índice interessante de ser verificado, uma vez que esta função é recente no organograma das empresas. O perfil outros (11,32%) é composto de coordenador de tecnologia e segurança, coordenador de informática e administrador de rede.

5.2 Política de Segurança da Informação: Importância

Os incidentes de segurança podem causar impacto nos negócios, uma vez que abalem um dos três pilares da segurança da informação (confidencialidade, integridade e disponibilidade). Os respondentes em geral percebem que o impacto na competitividade da empresa é maior caso ocorram incidentes de segurança que tornem indisponíveis as informações (média = 4,58). Esse impacto é considerado um pouco menor, caso ocorra alteração das informações (média = 4,55) e quebra de confidencialidade das informações (média = 4,38). Os resultados obtidos possuem uma média alta (tabela 3), mostrando que as empresas podem já ter percebido que os incidentes de segurança prejudicam o andamento dos negócios.

Tabela 3 - Impacto dos Incidentes de Segurança na Competitividade das Empresas

Tem Política	Quebra de Confidencialidade da Informação	Alteração das Informações	Indisponibilidade das Informações
Sim	4,48	4,48	4,55
Em desenvolvimento	4,21	4,86	4,86
Não	4,30	4,30	4,30
Conjunto	**4,38**	**4,55**	**4,58**

Escala Likert – 1 (muito baixo) a 5 (muito alto)

Com a aplicação do teste t nos resultados apresentados na tabela 3, chega-se a seguinte avaliação: no item alteração das informações, comparando-se as médias das categorias "possui política de segurança" e "está em desenvolvimento", a diferença é significativa (m1 = 4,48; m2 = 4,86; t = 2,284; p = 97,38%); na comparação das médias das categorias "não possui política de segurança" e "está em desenvolvimento", no item alteração das informações, a diferença é significativa (m1 = 4,86; m2 = 4,30; t = 2,110; p = 95,57%) e no item indisponibilidade das informações, a diferença é significativa (m1 = 4,86; m2 = 4,30; t = 2,110; p = 95,57%). Em todas as demais comparações a diferença entre as médias não é significativa.

Existem diversas maneiras de se proteger contra os incidentes de segurança. Segundo a NBR/ISO17799, dentro das boas práticas de segurança da informação estão a adoção de uma política de segurança, a realização de análises de riscos, a implantação de ferramentas de segurança, o desenvolvimento de planos de continuidade do negócio e o gerenciamento de riscos do ambiente. Os resultados apresentados na tabela 4 mostram que as empresas consideram a adoção de uma política de segurança como a mais importante medida para a prevenção de incidentes de segurança. Mesmo que não tenham consciência, as empresas consideraram importantes as boas práticas de segurança da informação recomendadas pela NBR/ISO17799, uma vez que nenhuma das medidas apresentadas para evitar incidentes de segurança obteve média inferior a 4,00.

Tabela 4 - Medidas para Evitar Incidentes de segurança

Tem Política	Análise de Risco	Política de Segurança	Implantação de Ferramentas de Segurança	Plano de Continuidade do Negócio	Gerência de Risco
Sim	29 (4,31)	29 (4,55)	29 (4,28)	29 (4,14)	29 (4,28)
Em desenvolvimento	14 (4,36)	14 (4,71)	14 (4,43)	14 (4,57)	14 (4,57)
Não	10 (4,10)	10 (4,30)	10 (4,30)	10 (4,10)	10 (4,20)
Conjunto	**53 (4,28)**	**53 (4,55)**	**53 (4,32)**	**53 (4,25)**	**53 (4,34)**

Número de respostas e Escala Likert – 1 (pouco importante) a 5 (muito importante)

Com a aplicação do teste t nos resultados obtidos na tabela 4, chega-se a seguinte avaliação: na comparação das médias das categorias "possui política de segurança" e "está em desenvolvimento" no item Plano de Continuidade dos Negócios, a diferença é pouco significativa (m1 = 4,14; m2 = 4,57; t = 1,489; p = 85.96%); na comparação das médias das categorias "não possui política de segurança" e "está em desenvolvimento" no item Política de Segurança da Informação, a diferença é pouco significativa (m1 = 4,71; m2 = 4,30; t = 1,757; p = 91,06%). Em todas as demais comparações a diferença entre as médias não é significativa.

Os ativos da informação possuem valor para a empresa e um incidente de segurança pode gerar um grande impacto para a organização. Desta forma, verifica-se que no resultado da tabela 5 a política de segurança é muito importante para proteger as informações do planejamento estratégico das empresas que já a possuem (média = 4,24) e para as empresas que ainda não a possuem (média = 4,30). Por outro lado, as empresas que estão desenvolvendo-a, consideram a política de segurança mais importante para controlar ativos e atividades que necessitem de informação. Cabe ressaltar que o roubo de informações confidenciais, de acordo com as pesquisas *Global Information Security Survey* (KPMG, 2002), é um dos maiores causadores de prejuízos financeiros e mesmo assim, as empresas que não possuem política de segurança consideraram o item de menor importância a proteção de marcas e patentes (média = 3,22).

Tabela 5 - Importância da Política de Segurança para os Aspectos Organizacionais

Tem Política	Exigência da governança Corporativa	Proteger Marcas e Patentes	Suportar a Estratégia Competitiva	Proteger as Informações do Planejamento Estratégico	Suprir Exigências Legais	Controlar ativos e atividades que necessitem de informação
Sim	27 (4,07)	28 (4,07)	29 (4,17)	29 (4,24)	28 (4,18)	29 (4,07)
Em desenvolvimento	14 (3,36)	13 (3,46)	14 (4,21)	14 (4,14)	14 (3,93)	14 (4,29)
Não	10 (3,80)	9 (3,22)	10 (4,00)	10 (4,30)	10 (3,80)	10 (4,00)
Conjunto	**51 (3,82)**	**50 (3,76)**	**53 (4,15)**	**53 (4,23)**	**52 (4,04)**	**53 (4,11)**

Número de respostas e Escala Likert – 1 (pouco importante) a 5 (muito importante)

Os resultados do teste t foram os seguintes para a comparação das médias entre as diversas categorias: na comparação das médias das categorias "possui política de segurança" e "não possui política de segurança", no item proteger marcas e patentes, a diferença é significativa (m1 = 4,07; m2 = 3,22; t = 2,072; p = 95.66%); na comparação das médias das categorias "possui política de segurança" e "está em desenvolvimento", no item suprir exigências da Governança Corporativa, a diferença é significativa (m1 = 4,07; m2 = 3,36; t = 2,244; p = 97.09%); no item proteger marcas e patentes, a diferença é pouco significativa (m1 = 4,07; m2 = 3,46; t = 1,709; p = 90.84%). Em todas as demais comparações a diferença entre as médias não é significativa.

Uma vez apresentada a importância da política de segurança, parte-se para a análise do seu processo de elaboração, implantação e manutenção.

5.3 Política de Segurança da Informação: Elaboração, Implantação e Manutenção

Para a elaboração de uma política de segurança é necessária a adoção de uma metodologia, seja ela proprietária ou normas internacionais e nacionais. Das empresas que possuem política de segurança (29), apenas 27,59% utilizou a NBR/ISO17799 como metodologia para o seu desenvolvimento. A maioria das empresas (58,63%) utilizou metodologia proprietária para a elaboração. Isto pode ter ocorrido uma vez que a ISO17799 só foi publicada em 2000 e antes dela não existia um padrão internacional para a gestão da

segurança da informação. Além disso, 6,90% utilizou outras metodologias que não foram especificadas e 6,90% não sabiam qual metodologia tinha sido utilizada, mesmo sendo esta pesquisa direcionada aos responsáveis pela segurança da informação nas empresas.

Já nas empresas que não possuem uma política de segurança ou estão desenvolvendo-a, 70,83% utilizariam a NBR/ISO17799 como metodologia para o processo de elaboração da política de segurança da informação, conforme apresentado na tabela 6. Apenas, 8,33% dessas empresas utilizariam uma metodologia proprietária. Esta grande parcela de possível adoção da NBR/ISO17799, pode ter ocorrido devido a maior divulgação da ISO17799 e da homologação da versão brasileira apresentada pela ABNT no ano de 2001.

Tabela 6 - Metodologia a ser Utilizada na Elaboração da Política de Segurança

Metodologia / Tem Política	NBR/ISO17799	Metodologia Proprietária	Outras	Não Sabe	Total
Em desenvolvimento	33,33% (8)	8,33% (2)	8,33% (2)	8,33% (2)	**58,33% (14)**
Não	37,50% (9)	0,00% (0)	0,00% (0)	4,17% (1)	**41,67% (10)**
Total	**70,83% (17)**	**8,33% (2)**	**8,33% (2)**	**12,50% (3)**	**100%**

Além da definição de uma metodologia para o desenvolvimento da política de segurança, é necessário no processo de sua elaboração que seja realizada, primeiramente, uma Análise de Risco dos Ativos da Informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001). Das empresas que possuem política de segurança (29) apenas duas não realizaram uma análise de risco. Isto pode indicar que apesar das empresas não terem adotado a NBR/ISO17799 como metodologia, elas acabam seguindo uma das boas práticas recomendadas pela norma que é a realização de uma Análise de Risco. Percebe-se também que os itens mais citados na composição da Análise de Risco foram: a identificação das ameaças e vulnerabilidade aos ativos da informação (24 citações) e a análise de impacto no negócio (24 citações). No entanto, a apresentação de solução para a correção dos problemas encontrados foi citada por apenas 17 empresas, o que pode causar um transtorno para as organizações, pois apesar de saberem as ameaças, os riscos e as vulnerabilidades, não foram orientadas em como resolvê-los ou minimizá-los.

Os itens constantes na tabela 7 devem fazer parte da Análise de Risco, de acordo com a NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001). Constatou-se, porém que apenas 12 empresas apresentaram todos os cinco itens em sua Análise de Risco, 6 empresas apresentaram 4 desses itens, 6 empresas apresentaram 3 itens, 3 empresas apresentaram 2 itens, e 2 empresas não apresentaram nenhum item, uma vez que não realizaram a Análise de Risco.

Tabela 7 - Itens Abordados na Análise de Risco

Itens da Análise de Risco	Citações	%
Identificação dos Ativos da Informação	22	20,00%
Identificação das ameaças e vulnerabilidade aos ativos da informação	24	21,82%
Avaliação da probabilidade de ocorrências das ameaças e vulnerabilidade aos ativos da informação	21	19,09%
Análise de Impacto no Negócio	24	21,82%
Solução para a correção dos problemas encontrados	17	15,45%
Não foi realizada uma análise de risco	2	1,82%
Total	110	100,00%

Já as empresas que não possuem política de segurança ou estão desenvolvendo-a, consideram, em conjunto, muito importante todos os itens apresentados pela norma NBR/ISO17799, em um processo de Análise de Risco. Cabe salientar a alta média do grau de

importância alcançada pelo item identificação das ameaças e vulnerabilidades, conforme visto na tabela 8. Para as empresas que não possuem uma política de segurança a média foi de 4,90 e para as empresas que estão desenvolvendo a média foi de 4,79.

Tabela 8 - Importância dos Itens Abordados na Análise de Risco

Importância dos Itens da Análise de Risco	Está em Desenvolvimento	Não	Conjunto
Identificação dos Ativos da Informação	4,36	4,50	**4,42**
Identificação das ameaças e vulnerabilidade aos ativos da informação	4,79	4,90	**4,83**
Avaliação da probabilidade de ocorrências das ameaças e vulnerabilidade aos ativos da informação	4,64	4,40	**4,54**
Análise de Impacto no Negócio	4,71	4,60	**4,67**
Solução para a correção dos problemas encontrados	4,29	4,30	**4,29**

Escala Likert – 1 (pouco importante) a 5 (muito importante)

O teste t foi aplicado para a comparação das médias da tabela 8 e os resultados obtidos foram os de que a diferença entre a médias não é significativa considerando uma significância de 5%.

A norma NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001) apresenta alguns elementos necessários que devem constar na política de segurança da informação, conforme apresentado na tabela 9. As empresas que possuem uma política de segurança, assinalaram a definição de responsabilidade (26 citações) e a apresentação da definição de segurança da informação (25 citações) como os dois itens que estão presentes na maioria das políticas de segurança. O item outros é composto por: palestras para novos colaboradores no momento de ingressar na empresa.

Os cinco primeiros itens apresentados na tabela 9 são recomendados pela NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001) para comporem a política de segurança da informação. Porém somente 6 empresas apresentam todos os itens em sua política de segurança. Onze empresas possuem 4 elementos, 4 empresas possuem 3 itens, 5 empresas possuem 2 itens e 3 empresas possuem apenas um item.

Tabela 9 - Itens que integram a Política de Segurança

Itens da Política de Segurança	Citações	%
Apresentação da definição de segurança da informação	25	25,00%
Definição de Responsabilidades	26	26,00%
Referências a procedimentos e regras de usuários	21	21,00%
Carta do Presidente	8	8,00%
Explanação de Políticas Específicas	19	19,00%
Outros	1	1,00%
Total	100	100,00%

As empresas que não possuem a política de segurança ou ainda estão desenvolvendo-a, consideram em conjunto a definição de responsabilidades como o item mais importante para estar presente na política de segurança, com média de 4,67, conforme apresentado na tabela 10.

Tabela 10 - Importância dos Itens que integram a Política de Segurança

Itens da Política de Segurança	Está em Desenvolvimento	Não	Conjunto
Apresentação da definição de segurança da informação	4,36	4,00	**4,21**
Definição de Responsabilidades	4,71	4,60	**4,67**
Referências a procedimentos e regras de usuários	4,36	4,30	**4,33**
Carta do Presidente	4,21	4,10	**4,17**
Explanação de Políticas Específicas	4,36	4,00	**4,21**

Escala Likert – 1 (pouco importante) a 5 (muito importante)

O teste t foi aplicado para a comparação das médias da tabela 10 e o resultado foi de que a diferença na comparação entre as médias não é significativa, considerando uma significância de 5%.

Uma vez analisados os itens que compõem a política de segurança, parte-se para a apresentação e discussão de um item específico, as políticas específicas. As políticas específicas são recomendadas pela NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001), e os itens apresentados na tabela 11 devem ser contemplados por elas. Verifica-se que o item conseqüências da violação da política de segurança (25 citações) é o que mais está presente nas políticas específicas. O menos presente é o requerimento de treinamento em segurança da informação aos colaboradores da empresa (16 citações).

Tabela 11 - Itens presentes nas Políticas Específicas

Itens das Políticas Específicas	Citações	%
Conformidade com a legislação e cláusulas contratuais	22	19,82%
Requerimentos de treinamento em segurança da informação aos colaboradores da empresa	16	14,41%
Detecção e prevenção de vírus e software malicioso	24	21,62%
Gestão da Continuidade do Negócio	24	21,62%
Conseqüências da violação da política de segurança	25	22,52%
Não existem políticas específicas	0	0,00%
Total	111	100,00%

As empresas que não possuem política de segurança ou estão desenvolvendo-a avaliaram o grau de importância dos itens que compõem as políticas específicas. Desta forma, constatou-se que o a gestão da continuidade do negócio é o item que apresenta a maior média em conjunto (média = 4,65), conforme apresentado na tabela 12. Também é importante salientar que dois requisitos importantes para o processo de implantação da política de segurança, apresentam as médias mais baixas, são eles: conformidade com a legislação e cláusulas contratuais (média = 4,04) e requerimentos de treinamento em segurança da informação aos colaboradores da empresa (média = 4,04). Este último item é considerado de baixa importância pelas empresas que não possuem política de segurança e pelas que estão desenvolvendo uma e também é o item menos presente nas políticas de segurança das empresas que já a possuem.

Tabela 12 - Importância dos Itens presentes nas Políticas Específicas

Tem política	Em desenvolvimento	Não	Conjunto
Conformidade com a legislação e cláusulas contratuais	4,00	4,10	**4,04**
Requerimentos de treinamento em segurança da informação aos colaboradores da empresa	4,23	3,80	**4,04**
Detecção e prevenção de vírus e software malicioso	4,31	4,40	**4,35**
Gestão da Continuidade do Negócio	4,79	4,40	**4,63**
Conseqüências da violação da política de segurança	4,64	4,30	**4,50**

Escala Likert – 1 (pouco importante) a 5 (muito importante)

Foi realizado o teste t para a comparação das médias apresentadas na tabela 12 e o resultado obtido foi o seguinte: no item Gestão da Continuidade dos Negócios a diferença entre as médias é pouco significativa (m1 = 4,79; m2 = 4,40; t = 1,499; p = 85,54%), considerando um risco de 5%. Nos demais itens a diferença entre as médias não é significativa.

Com a política de segurança elaborada, as empresas partem para o processo de divulgação e conscientização dos colaboradores da empresa, a fim de realizar a implantação da política de segurança. Nota-se, que somente uma empresa ainda não implantou a sua política de segurança, conforme apresentado na tabela 13. Por outro lado, as empresas que já implantaram utilizaram-se primeiramente de materiais de divulgação como folders e cartazes (22 empresas), entregaram cópias da política de segurança (20 empresas). No entanto, somente 16 empresas fizeram os colaboradores assinarem um termo de responsabilidade e poucas empresas utilizaram as palestras de conscientização (14 empresas) e os treinamentos específicos na política (12 empresas). O item outros é composto das seguintes ações: publicação na Intranet sobre a política de segurança; mensagem de correio eletrônico explicativa sobre o processo de segurança, comunicação individual dos processos de segurança da informação.

Tabela 13 - Ações utilizadas para a Implantação da Política de Segurança

Implantação da Política de Segurança	Citações	%
Palestras de Conscientização	14	15,91%
Treinamento específico na política de segurança	12	13,64%
Folders e cartazes	22	25,00%
Entrega de cópias da política de segurança	20	22,73%
Assinatura de termo de responsabilidade	16	18,18%
Outros	3	3,41%
Nenhum	0	0,00%
A política ainda não foi implantada	1	1,14%
Total	88	100,00%

No processo de implantação da política de segurança as empresas que não possuem uma política de segurança e as que ainda estão desenvolvendo-a, gostariam de utilizar primeiramente as palestras de conscientização (24 empresas), seguido da assinatura do termo de responsabilidade (23 empresas), conforme descrito na tabela 14. Isto mostra um contraste perante as ações utilizadas pelas as empresas que já possuem uma política de segurança.

Tabela 14 - Itens que devem ser utilizados para a Implantação da política de Segurança

Tem política	Em desenvolvimento	Não	Conjunto
Palestras de Conscientização	14	10	**24**
Treinamento específico na Política de Segurança	10	8	**18**
Folders e Cartazes	7	6	**13**
Entrega de cópias da Política de Segurança	11	7	**18**
Assinatura de termos de responsabilidade	14	9	**23**
Outros	1	0	**1**
Total	57	40	**97**

Segundo a NBR/ISO17799 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001) é necessário que exista um processo para a revisão da política de segurança. Conforme apresentado na tabela 15, as empresas estão realizando essas revisões da política, em sua maioria, a cada 12 meses (9 empresas). Mesmo sendo esta pesquisa direcionada aos responsáveis pela segurança da informação na empresa, dois respondentes não souberam precisar a periodicidade da revisão da política de segurança. O item outro é composto por: conforme a necessidade de atualização.

Tabela 15 - Periodicidade das Revisões da Política de Segurança

Periodicidade	Citações	%
A cada 3 meses	7	21,14%
A cada 6 meses	5	17,24%
A cada 12 meses	9	31,03%
Indeterminado	3	10,34%
Outro	3	10,34%
Não sabe	2	6,90%
Total	29	100,00%

Conforme apresentado na tabela 16, a revisão da política de segurança deve ocorrer a cada 6 meses. Esta é a opinião em conjunto das empresas que estão desenvolvendo a política de segurança (7 citações) e as que não possuem (6 citações).

Tabela 16 - Opinião da Periodicidade das Revisões da Política de Segurança

Opinião de Periodicidade	Em desenvolvimento	Não	Total
A cada 3 meses	28,57% (4)	0,00% (0)	**16,67% (4)**
A cada 6 meses	50,00 (7)	60,00% (6)	**54,17% (13)**
A cada 12 meses	7,14% (1)	10,00% (1)	**8,33% (2)**
Indeterminado	7,14% (1)	20,00% (2)	**12,50% (3)**
Não sabe	7,14% (1)	10,00 (1)	**8,33% (2)**
Total	100,00% (14)	100,00% (10)	**100,00 % (24)**

Conforme descrito na tabela 17, a maioria das empresas que já possuem uma política de segurança (34,48%) já realizaram de 1 a 3 revisões de sua política de segurança. Salienta-se que seis empresas ainda não realizaram nenhuma revisão. Isto pode ocorrer, uma vez que a política de segurança é recente ou também pode mostrar que o processo de revisão não está corretamente implantado. Além disso, existem 3 empresas que não sabem quantas revisões foram realizadas. Neste caso, ou o processo de revisão não foi implementado ou se foi, não existem procedimentos e documentos para a anotação das revisões, suas datas e responsáveis.

Tabela 17 - Quantidade de Revisões da Política de Segurança

Quant. de Revisões	Citações	%
De 1 a 3 revisões	10	34,48%
De 4 a 6 revisões	7	24,14%
Mais de 6 revisões	3	10,34%
nenhuma	6	20,69%
Não sabe	3	10,34%
Total	29	100,00%

6 Conclusões

Com a análise dos resultados, constata-se a percepção dos diretores de tecnologia, gerentes de tecnologia e *security officers* das empresas que participaram da pesquisa que possuem política de segurança, que não a possuem ou estão desenvolvendo-a sobre os aspectos abordados nesta pesquisa. Em geral, as empresas percebem que um incidente de segurança, que cause a indisponibilidade das informações, a quebra de sua confidencialidade e que permita que as mesmas sejam alteradas sem autorização, pode causar impacto na competitividade da organização no mercado. Uma vez que as empresas reconhecem os riscos aos quais estão expostas, o desenvolvimento da política de segurança se torna um caminho natural no processo de gestão da segurança da informação. Isso foi demonstrado uma vez que a maioria das empresas já possui uma política de segurança ou estão desenvolvendo-a. A proteção das informações do planejamento estratégico, o suporte à estratégia competitiva e o

controle dos ativos e atividades que necessitem de informação são os aspectos organizacionais mais importantes que a política de segurança deve proteger.

O processo de elaboração, implantação e manutenção da política de segurança com as recomendações da NBR/ISO17799 é relativamente novo, por isso a maioria das empresas que já possuem a política de segurança não utilizou a NBR/ISO17799 como metodologia para o seu desenvolvimento. No entanto, as empresas que estão desenvolvendo-a e as que não possuem utilizariam a norma para elaborar a sua política de segurança. É importante salientar as empresas que não adotaram a norma como metodologia, mesmo assim, em sua maioria seguiram as boas práticas no processo de elaboração, realizando uma Análise de Risco. Além disso, identificou-se empresas que apresentaram todos os itens recomendados pela norma em uma Análise de Risco.

As empresas consideraram de grande importância a adoção de todos os itens da NBR/ISO17799 referentes à composição da política de segurança. Dentre esses itens, destaca-se a definição das responsabilidades, pois obteve o maior índice de importância e é o mais presente nas políticas de segurança já desenvolvidas. Isto mostra, que a política está sendo usada para organizar as relações entre as pessoas e os ativos na organização. Além disso, na explanação das políticas específicas, a preocupação com a detecção de vírus e software maliciosos destaca-se como o item mais importante e o mais presente nas políticas de segurança. Isto mostra a preocupação com um dos tipos mais freqüentes de incidentes de segurança que são os ataques de vírus.

Sabe-se que as mudanças organizacionais, normalmente devem transpor barreiras culturais impostas pelo desconhecimento dos objetivos dessas mudanças. A implantação da política de segurança é um fator crítico para a organização e por isso é importante um grande trabalho de divulgação e conscientização dos colaboradores. Os resultados mostram a adoção de diversas atividades que podem auxiliar neste trabalho, sendo os mais utilizados os folders e cartazes. Porém as empresas que ainda não implantaram a sua política de segurança utilizariam, em sua maioria, as palestras de conscientização. Comparando com as recomendações da NBR/ISO17799 as empresas em geral estão adotando ou adotariam diversas ações em conjunto como palestras de conscientização, assinatura de termos de responsabilidade, folders e cartazes e entregas de cópias da política de segurança no processo de implantação.

Já o que se refere à manutenção da política de segurança a maioria das empresas possuem um cronograma de revisão que varia de “a cada 3 meses” até “a cada 12 meses”. Também constatou-se que as políticas já foram revisadas algumas vezes, mostrando que o processo de manutenção está ocorrendo, conforme recomendado pela NBR/ISO17799.

Sugere-se para as empresas que já estão desenvolvendo ou que pretendem desenvolver sua política de segurança, que sejam adotadas as boas práticas recomendadas pela NBR/ISO17799. Desta forma, a empresa poderá adotar o processo de gestão da segurança da informação e de acordo com uma norma internacional, aplicada e reconhecida como as melhores práticas. E para as empresas que já elaboraram suas políticas de segurança recomenda-se que em seu plano de revisões sejam realizadas as adequações necessárias para estarem de acordo com a norma.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR/ISO 17799:** código de práticas para a gestão de segurança da informação. Rio de Janeiro, 2001.

BALARINE, O. F. O. Tecnologia da informação como vantagem competitiva. **RAE Eletrônica**, São Paulo, n. 1, a. 1, jan./jun. 2002.

BASTOS, A. Os novos rumos da gestão de segurança com as normas ISO17799 e BS 7799. **Módulo Security Magazine,** Rio de Janeiro, ago. 2002.

BONCELLA, R. Wireless Security: an overview. **In. Eighth Americas Conference on Information Systems**, 2002. CD-ROM.
BRITISH STANDARD. **BS7799-2:2002** – Information security management systems – specification with guidance for use. Inglaterra, ago. 2002.
BSI. **ISO17799 – If your information's not safe, your future's not secure**. Disponível em:<http:// www.bsiamericas.com>. Acesso em: 02 out. 2002.
CAVUSOGLU, H.; MISHRA, B.; RAGHUNATHAN, S. Assessing the value of detective control in IT security**. In. Eighth Americas Conference on Information Systems**, 2002. CD-ROM.
DHILLON, G.; BACKHOUSE, J. Current directions in IS security research: towards socio-organizational perspectives. **Journal of Information Systems**, n. 11, p. 127-153, 2001.
DIPPEL, T. IT as an enabler of computer fraud. **Information Security Technical Report**. XX, v. 5, n. 2, p. 60-70, 2000.
E-TRUST. **Política de Segurança**. Disponível em <http:// www.e-trust.com.br>. Acesso em: 12 jun. 2002.
FREITAS, H.; LESCA, H. Competitividade empresarial na era da informação. **RAE – Revista de Administração de Empresas.** São Paulo, v. 27, n. 3, p. 92-102, jul./set. 1992.
KPMG. **Global information security survey 2002**. Disponível em: <http://www.kpmg.com>. Acesso em: 20 maio 2002.
LAUDON, K.; LAUDON, J. **Sistemas de informação**. 4. ed. Rio de Janeiro: LTC, 1999.
LAUDON, K.; LAUDON, J. **Management Information Systems:** organization and technology in the networked enterprise. 6. ed. New Jersey: Prentice Hall, 2000.
MALHOTRA, N. K. **Pesquisa de marketing:** uma orientação aplicada. 3. ed. Porto Alegre: Bookman, 2001.
MASON, T. Platform security and commom criteria. **Information Security Technical Report**. XX, v. 5, n. 1, p. 14-25, 2000.
MÓDULO. **Oitava pesquisa nacional de segurança da informação**, set. 2002.
NAKAMURA, E.T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Berkeley Brasil, 2002.
NAVARRO, L. Information security risks and managed security services. **Information Security Technical Report**. XX, v. 6, n. 3, p. 28-26, 2001.
O'BRIEN, J. **Sistemas de informação e as decisões gerenciais na era da Internet**. 9. ed. São Paulo: Saraiva, 2001.
PATRICK, W.F. Creating an information systems security policy. **SANS Institute**. Disponível em: <http://rr.sans.org/policy/infosys.php>. Acesso em: 18 mar. 2002.
PORTER, M. **Vantagem competitiva:** criando e sustentando um desempenho superior. 19. ed. Rio de Janeiro: Campus, 1989.
POWER, R. 2002 CSI/FBI Computer Crime and Security Survey**. Computer Security Issues e Trends**, San Francisco, v.8, n. 1, 2002.
RASHBAUM, W.K. Forum in New York: Computer Security. **In: World Economic Forum**, New York, 2002.
REGISTER INTERNATIONAL. Disponível em <www.xisec.com>. Acesso em: 10 nov. 2002.
ROCHA. Acusação de roubo de base de dados agita web brasileira. **Portal Módulo**, 2002. Disponível em: <http://www.modulo.com.br >. Acesso em: 20 dez. 2002.
TREGEAR, J. Risk Assessment. **Information Security Technical Report**. XX, v. 6, n. 3, p. 19-27, 2001.
URCUYO, C.E.; KUNNATHUR, A. knowledge sharing strategy: the significance of security and collaboration. **In: Eighth Americas Conference on Information Systems**, 2002. CD-ROM.

WILLIAMS, P. Information Security Governance. **Information Security Technical Report**, v. 6, n. 3, p. 60-70, 2001.
YAPP, P. Who's bugging you? How are you protection your information? **Information Security Technical Report**, v. 5, n. 2, p. 23-33, 2000.

[1] Os autores agradecem o fundamental apoio do CNPq e da Fapergs.