Formação de Redes entre Empresas: Análise de Modelos de Segurança das Informações.

Flávia Vancim Frachone Neves (USP) flavancin@gmail.com
Fábio Muller Guerrini (USP) fabmg@prod.eesc.usp.br

Resumo
No cenário atual da economia brasileira, as pequenas e médias empresas (PME's) de diversos setores produtivos procuram estabelecer parcerias para sanar deficiências, entre as quais destacam-se: falta de apoio governamental, infra-estrutura inadequada, tecnologia ultrapassada, ausência de investimentos em pesquisa e desenvolvimento, carência de mão-de-obra qualificada, ou seja, limitação de recursos técnicos, humanos e financeiros. Em função disto, a possibilidade de formação de redes entre PME's têm emergido como a alternativa viável e promissora de impulsionar o mercado. No entanto, apesar da parceria entre PME's ser uma solução adequada para a crise econômica vivenciada na atualidade, existe a barreira da falta de confiança mútua entre os parceiros de cooperação, além de outros fatores comportamentais e tecnológicos que interferem diretamente na consolidação dessas redes. Diante do exposto, este trabalho analisa os problemas comportamentais existentes em ambientes cooperativos, bem como os mecanismos de segurança das informações viáveis para a formação e desenvolvimento das redes de cooperação.
Palavras Chave: Cooperação; Segurança; Informação.

1. Introdução

As pequenas e médias empresas (PME's) enfrentam dificuldades, tanto de ordem financeira quanto de recursos humanos e técnico-organizacionais limitados, que as impede de se tornarem competitivas frente às economias internacionais, nacionais e até mesmo regionais. No entanto, essas dificuldades podem ser amenizadas se as PME's associarem-se na forma de "sistemas cooperativos".

A cooperação significa que um grupo de empresas interagem trocando competências que vão além do puro relacionamento puro de compra e venda. De acordo com Bremer (2000), a relação entre essas empresas não se restringe a ajudar ou apoiar uma a outra mas, sim, realizar as atividades conjuntamente.

Neste contexto, Casarotto e Pires (2001) afirmam que a cooperação entre pequenas e médias empresas é algo tão irreversível como a globalização, ou melhor, talvez seja a maneira como as PME's possam assegurar sua sobrevivência e a sociedade garantir seu desenvolvimento equilibrado. Adicionalmente, Amato (2000) reporta que a formação das redes de cooperação pode ser vista como uma solução viável para as PME's, que se encontram em desvantagem frente às grandes empresas, uma vez que, no geral, estas possuem condições suficientes de dominar todas as etapas da cadeia de valor (produção, pesquisa e desenvolvimento, tecnologia de gestão, logística de distribuição e marketing).

2. Formação das Redes de Cooperação: Vantagens e Desvantagens

As redes interempresariais apresentam-se como alternativa viável e promissora para a sobrevivência e desenvolvimento das pequenas e médias empresas brasileiras. Diante disto, torna-se interessante discutir as vantagens e desvantagens na formação dessas redes.

Segundo Amato (2000), a constituição de uma rede de cooperação viabiliza, às organizações, entre outros fatores, a:

- Permitir a definição de estratégias conjuntas: pois as empresas estarão cooperando umas com as outras;
- Preservar a individualidade e proteção de dados: pois cada empresa estará disponibilizando seu "produto final", e não seus recursos;
- Valorizar marcas e possibilitar o marketing compartilhado: as campanhas publicitárias serão desenvolvidas para a rede, e, desta forma, estarão melhorando a comunicação com os consumidores para fortalecer a marca e firmar um conceito comum;
- Reduzir custos de produção e riscos de investimentos: já que o mesmo será dividido com todas as empresas da rede;
- Intensificar a comunicação e o acesso à informação: a interconexão entre as empresas leva a uma intensificação do processo de comunicação, e, conseqüentemente, à maior riqueza das fontes de informação;
- Ampliar a escala produtiva e dimensões de mercado: a cooperatividade viabiliza maior escala de produção a um custo e tempo menores, possibilitando às empresas explorar outros mercados;
- Facilitar o acesso ao crédito e à capacitação gerencial: empresas reunidas possuem maior poder de negociação, facilidade em linhas de crédito, maior credibilidade pelo número de empresas envolvidas, além de disponibilizar um nivelamento de conhecimento gerencial para melhorar e aprimorar o planejamento estratégico da rede.

Entretanto, como desafios à formação das redes de cooperação há os obstáculos de se conseguir, na prática, mútua confiança entre as empresas, tendo em vista que esse aspecto possui grande relevância na manutenção e sobrevivência das mesmas.

O sentido da confiança, ainda segundo Amato (2000), é de essencial importância no mundo dos negócios, pois todas as transações econômicas envolvem riscos, não somente relacionados com possíveis fraudes, como também à imprevisibilidade dos acontecimentos futuros. Estes riscos, se não controlados, podem impedir a concretização de negócios que trariam benefícios para todas as partes.

Nota-se, também, que pequenas e médias empresas possuem excessiva preocupação com o "curto prazo" e, assim, postergando investimentos que poderiam gerar opções de futuro crescimento a empresa. A decisão da organização em atuar cooperativamente pressupõe que a mesma esteja disposta a compartilhar informações e conhecimentos estratégicos, pois, como coloca Carreto (2002), se a integração entre empresas resulta numa série de benefícios, por outro lado, essa relação pode se desfazer. Neste caso, as firmas que compunham a rede passam a ter como concorrentes suas antigas cooperadas, as quais possuem todo o conhecimento sobre suas antigas aliadas. Dessa forma, pode-se instaurar o dilema entre cooperação e competição, fator ao qual também podem-se atribuir a "responsabilidade" pelo entrave à formação de redes.

3. Aspectos Comportamentais nos Ambientes Cooperativos

As organizações, de modo geral, ficam cada vez mais preocupadas com suas aparentes incapacidades de tratar, compreender, manipular a expressiva quantidade e diversidade de dados que toma conta de tudo. O próprio volume disponível de informação torna parte dela

inutilizável, devido à incapacidade de usá-la adequadamente e pela forma como ela é transmitida.

Para compreender qualquer tipo de informação nova é necessário, primeiramente, possuir algum interesse em recebê-la, bem como descobrir a estrutura em que ela esteja ou deveria estar organizada e examiná-la sob diferentes perspectivas. Entretanto, o pré-requisito essencial para a compreensão, segundo Wurman (1995), é sermos capazes de admitir ignorância quando não houver entendimento sobre algo pois, desta forma, estaremos mais "relaxados" e, conseqüentemente, mais abertos a formular perguntas e a receber a informação nova.

A recusa em admitir ignorância nos atrapalha e, coletivamente, é dela a responsabilidade primária pela ansiedade e pela frustração que as pessoas têm diante da necessidade de se manterem informadas. Ou seja, as pessoas ficam ansiosas com a sensação de que devem saber tudo. Perceber as próprias limitações torna-se essencial para sobreviver a uma avalanche de informações.

Em contra partida, esse pré-requisito essencial para a compreensão é um conceito radical em nossa sociedade, pois existem poucas recompensas e muitas punições para o reconhecimento da ignorância tanto em nível pessoal quanto profissional. Adicionalmente, a relevância dada ao desafio e à competição, pela sociedade, aumenta, nas pessoas, a noção de que não é político ou, pelo menos, não é polido reconhecer a incompreensão.

Para enfrentar essa crescente proliferação de dados, é imperativo compreender o que se deve entender como informação. Wurman (1995) afirma que ela deve ser aquilo que leva à compreensão; além disto, há o fato da informação se caracterizar de uma forma para uma pessoa, e não passar de dados para outra.

Divergências entre dados e informação tornam-se mais expressivas, à medida que a economia mundial caminha para um sistema dependente de informação e comunicação.

Ideal seria se pudéssemos entregar, aos clientes, a informação de forma mais organizada, de forma a torná-la mais compreensível. No entanto, a ordem não necessariamente é a garantia de compreensão podendo, às vezes, ocorrer o contrário.

Com relação à comunicação, pode-se dizer, ainda segundo Wurman (1995), que existe três tipos de atividades relacionadas à difusão da informação: de transmissão, armazenamento e transmissão. Especificamente esta última refere-se à televisão, telégrafo, telefone, telex, e tudo mais que comece por "tele" e possa ser transmitido por fios, rebatidos por um satélite ou impressos em uma página.

Portanto, de acordo com Meadows (1991), informação e comunicação são essenciais à existência humana, pois podem prover estabilidade em suas relações comportamentais. Além disso, Pignatari (1970) interpreta a comunicação como modos de comportamento, ou seja, a relação estabelecida entre transmissão de estímulos e provocação de respostas. Adicionalmente, ressalta-se que a posse da informação reduz incertezas sobre algum estado ou evento.

Diante do exposto, vale ressaltar que a constante transição econômica acarreta, nas organizações de modo geral, a uma permanente necessidade de informação. Essa *ansiedade de informação*, segundo Wurman (1995), é o resultado da distância entre o que é compreendido e o que se acredita que deveria ser compreendido. Isso ocorre quando a informação não nos sacia, ou seja, não é suficiente. Além disso, a ansiedade é gerada, também, quando ocorrem tais situações: não compreender a informação; sentir-se assoberbado por seu volume; não saber se certa informação existe; não saber onde encontrá-la; nem exatamente onde ela situa-se. Ainda assim, essa ansiedade pode aumentar quando houver consciência do limite de acesso à informação e comunicação.

Contudo, pode-se, notoriamente, afirmar que a alta administração da empresa tem a responsabilidade de determinar a política de comunicação a ser instaurada, e criar um ambiente em que os empregados sejam encorajados a expor suas idéias. Para tanto, devem ser tomados alguns passos para estimular o diálogo produtivo com os funcionários. São eles:

1. Atenuar diferenças hierárquicas. O tamanho, e a posição dos escritórios dos executivos podem ser definidos de modo a criar maior proximidade entre o empregado e o executivo;
2. Incentivar empregados sérios, leais e francos. Se a organização tem um ou dois indivíduos aos quais esta definição se aplica, considere-se um proprietário de sorte, pois a coragem nunca foi endêmica nas organizações;
3. Estabelecer o tipo de linha de comunicação que, provavelmente, seus empregados provavelmente têm mantido há anos.

A necessidade de estratégia de desenvolvimento da cooperatividade interempresarial é essencial, principalmente para pequenas e médias empresa, como afirma Bremer (2000), cujos recursos e estímulos, comparados às grandes empresas, são limitados.

Por fim, empresas que desejam compor uma rede devem ser capazes de aprender com as experiências, uma vez que no mercado competitivo e dinâmico os ambientes de cooperação ainda são formas de organização em desenvolvimento.

4. Segurança das Informações na Rede em Ambientes Cooperativos

Analisar questões referentes à segurança das informações, que trafegam via *Internet*, das redes em ambientes cooperativos é um fator de grande relevância e não muito difundido dentro do conceito de formação de redes de cooperação entre PME's brasileiras.

De acordo com Nakamura e Geus (2002), as tecnologias da informação devem ser adotadas mediante uma política de segurança, que varia para cada rede, pois o ambiente cooperativo é complexo e a segurança necessária a ser implementada é igualmente complexa, envolvendo aspectos humanos, tecnológicos e sociais.

Com isso, com o propósito de trocar informações e economizar recursos, a rede de computadores dá lugar a um novo ambiente. Ainda segundo Nakamura e Geus (2002), a importância da *Internet* nos negócios e a globalização resultam em trocas de informações técnicas, comerciais e financeiras por meio de redes integradas entre empresas matrizes, filiais, fornecedores e parceiros comerciais.

Portanto, as informações agora são primordiais para o sucesso das negociações. Em virtude disso, o grau de proteção e preocupação com estas informações cresceu consideravelmente dentro deste ambiente integrado. Medidas e cuidados de segurança devem ser tomados e sempre verificados.

A segurança em ambientes cooperativos será, então, não apenas uma proteção das informações trafegadas pela rede, mas também o resultado do conjunto de esforços para entender o ambiente e as tecnologias, saber como utilizá-la e implementá-la de modo correto para viabilizar os negócios da organização.

4.1 – Planejamento das Necessidades de Segurança

A segurança dos dados tornou-se segurança do computador, que por sua vez tornou-se segurança dos sistemas de informação, que também por sua vez tornou-se segurança das informações devido ao melhor entendimento do impacto dos negócios e risco associado a não propriamente proteger os recursos eletrônicos da companhia. (SOLMS, 2005)

A segurança da informação tornou-se integral para um bom gerenciamento da corporação. Embora esse fato sempre tenha sido verdadeiro, apenas recentemente foi enfatizado no bom gerenciamento da corporação. Elevar a "segurança das informações" para a "segurança dos negócios", acrescerá foco extra às necessidades de assegurar a prolongada existência da companhia, e integrará e envolverá todos os presentes esforços, da mesma forma que a proteção será considerada.

Antes de se estabelecer qual a melhor política de segurança para a rede, faz-se necessário analisar e planejar qual a real necessidade da mesma pois, desta forma, implantações de mecanismos de segurança não serão adotados inadequadamente. O primeiro passo para melhorar a segurança de um sistema é, segundo Nakamura e Geus (2002), considerar alguns aspectos, entre os quais se destacam:

- Conhecer os possíveis inimigos, identificar o que eles desejam fazer e os perigos que podem vir a causar à organização;
- Contabilizar os valores, pois a implementação e o gerenciamento da política de segurança, além da necessidade de mais recursos pessoais, podem significar a necessidade de significativos recursos de software e de hardware. Os custos das medidas de segurança devem, portanto, ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança;
- Considerar os fatores humanos, pois muitos procedimentos de segurança falham porque as reações dos usuários a esses procedimentos não são consideradas com seu devido valor;
- Conhecer os pontos fracos, pois todo sistema tem suas vulnerabilidades;
- Compreender o ambiente da rede, para que seja possível detectar possíveis comportamentos estranhos, antes que um invasor cause prejuízos;
- Aplicar a segurança de acordo com os negócios da organização, a fim de definir uma estratégia de segurança que melhor se adapte às necessidades da mesma.

Dessa maneira pode-se ter conhecimento do que se tenta proteger, contra quem e quanto tempo e custo pretende-se gastar para obter a proteção adequada. Com isso, tem-se a base da análise de risco. A partir daí, pode-se planejar políticas e técnicas que serão necessárias para implementar e reduzir esses riscos.

Em contra partida, há de se concordar que o risco não pode ser totalmente eliminado pois, repentinamente, sempre pode surgir um risco secundário, sem que estejamos preparados para lidar com ele. Dessa forma, uma avaliação cuidadosa do risco principal, identificará estes riscos secundários, auxiliando, assim, a estabelecer planos de ação.

4.2 – Controle de Acesso em Redes

Em um sistema em rede, conforme expões Guttman (2004), muitos dispositivos, como: roteadores, *firewalls*, redes privadas virtuais etc, devem cooperar-se para atingir-se as metas de segurança. Estes dispositivos podem requerer diferentes configurações, dependendo de seus respectivos propósitos e localização na rede.

A propriedade determinante dos ambientes cooperativos entre organizações é a complexidade que envolve a comunicação entre diferentes tecnologias, diferentes usuários, diferentes culturas e políticas internas. O conjunto de protocolos TCP/IP e a *Internet* possibilitaram o avanço em direção aos ambientes cooperativos, ao tornar possíveis as conexões entre as diferentes organizações, de modo mais simples e barato. Porém, como coloca Nakamura e Geus (2002), essa interligação teve como conseqüência uma enorme implicação quanto à proteção dos valores de cada organização.

Algumas situações que refletem o grau de complexidade existente em ambientes cooperativos podem ser vistas quando são analisadas, por exemplo, as conexões entre as organizações componentes da rede de cooperação. Como proteger os valores de uma organização, evitando que um usuário de outra organização acesse informações que pertençam somente àquela e assim por diante?

Os problemas que aparecem quando isso ocorre são diversos, pois as organizações acabam por ter acesso a informações confidenciais, umas das outras, sem terem conhecimento. Outro fator está relacionado ao aumento da complexidade dos níveis de acesso que cada componente da rede poderá acessar de outros e vice-versa. Essa situação demonstra o grande desafio de controlar os acessos em diferentes níveis, que pode se tornar ainda mais complexo, se diferentes usuários de uma determinada organização necessitarem acessar diferentes recursos de outro membro da rede.

Em vista disso, apresentam-se três mecanismos de segurança das informações na rede viáveis para ambientes cooperativos entre PME's brasileiras.

- **Criptografia de Dados:** a vulnerabilidade dos dados ocorre no momento em que os mesmos são compartilhados na rede. Para tanto, a criptografia possui uma função e importância cada vez maior dentro das soluções de segurança, por garantir a confidencialidade, integridade, autenticação, certificação e não repúdio dos dados trafegados na rede.

  O mecanismo da criptografia baseia-se, sucintamente, em descrever as mensagens de forma que apenas o receptor consiga decifrá-la, pois a mensagem original é passada por um processo de codificação, gerando uma mensagem cifrada.

  Segundo Albertin (1998), a criptografia é a mutação de informação em qualquer forma (texto, vídeo ou gráficos) em uma representação não legível por qualquer pessoa que não possua a chave de decodificação da mensagem.

  No entanto, a criptografia não assegura que um intruso não: apague todos os dados, independentemente se estes estão ou não criptografados; modifique o programa para modificar a chave pois, desta forma, o receptor não conseguirá decriptografar a mensagem ou; até mesmo, acesse o arquivo antes de ele ser criptografado.

- **Tunelamento:** é uma técnica adequada a ser utilizado nas Redes Privadas Virtuais (VPN's) a fim de, juntamente com a criptografia, fornecer segurança no tráfego dos dados entre as organizações.

  Os protocolos de tunelamento, como expõem Nakamura e Geus (2002), utilizados nas VPN's, tratam do encapsulamento dos dados do usuário em pacotes IP. O tunelamento é importante, porque um túnel IP pode acomodar qualquer tipo de encapsulamento e o usuário pode utilizar a VPN para, de modo transparente, acessar a rede da organização, em qualquer base (IP, IPX, AppleTalk, etc.).

  Em caso de ambientes cooperativos, os túneis VPN's são criados na própria rede da organização. Para os usuários, é como se essas redes diferentes, na realidade, fossem uma única rede, constituindo assim a rede privada virtual, que passa fisicamente por uma rede pública.

- ***Firewall:*** é um sistema de segurança das informações que trafegam pelos canais da rede. Segundo Nakamura e Geus (2002), *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, pelo qual passa todo o tráfego, permitindo que sejam realizados o controle, a autenticação e os registros de todo o tráfego. Assim, esse ponto único geralmente constitui um mecanismo utilizado para proteger uma

rede confiável de uma rede pública não confiável. Ou seja, é um sistema ou grupo de sistemas que reforça a política de controle de acesso entre redes.

O *firewall* é composto por diversos componentes, pois cada um deles possui uma funcionalidade distinta, desempenhando um papel que influi diretamente no nível de segurança do sistema. Todo o tráfego originário da *Internet*, ou caminhando para ela, passa através do *firewall*. Desta forma, o mesmo tem a oportunidade de garantir que este tráfego seja aceitável, ou seja, aquilo que esteja sendo feito: e-mail, transferência de arquivos, login remoto ou qualquer outro tipo de interações específicas entre sistemas em conformidade com a política de segurança do *firewall*.

Adicionalmente, segundo Moreira e Cordeiro (2002), mais freqüentemente, um *firewall* é um conjunto de componentes de hardware: um roteador, um *host* ou uma combinação de roteadores, computadores e redes com o *software* apropriado.

Vale ressaltar que, apesar de ser considerado uma tecnologia "antiga", não pode ser tido como estável pois continua em permanente evolução, pois aumenta, cada vez mais, o nível de complexidade das redes das organizações. Adicionalmente, pode-se colocar que um dos grandes problemas do *firewall* deve-se ao fato de a falsa idéia de que ele seja a solução dos problemas de segurança pois, nos ambientes cooperativos, ele não pode ser considerado apenas um "muro" mas sim parte da defesa ativa das organizações.

Tratando-se de ambientes cooperativos salienta-se, ainda, que o *firewall* deve possuir excelente desempenho, pois a complexidade das conexões, somada ao grande conjunto de regras, exige um alto poder de processamento para a rápida análise de todos os pacotes trafegados na rede.

Alguns dos aspectos envolvidos em ambientes cooperativos são as diferenciações entre diversos usuários existentes, os desafios a serem enfrentados em um ambiente cooperativo e a complexidade das conexões desse ambiente.

Citando cada item já exposto, pode-se dizer que, em relação à diferenciação de usuários - uma vez que esses diferentes tipos de usuários passam a acessar cada vez mais os recursos internos das organizações - o mais prudente é não fazer essa diferenciação. A preocupação com a segurança deve ser tratada no nível interno das organizações. Ou seja, a segurança interna passa a ser essencial em ambientes cooperativos, a fim de garantir que os recursos sejam acessados por usuários autorizados.

No entanto, é difícil lidar com a complexidade gerada entre os diferentes níveis de acesso existentes, sem comprometer a segurança bem como seus integrantes pois, quando diversas conexões passam a se interconectar, torna-se maior o risco de interferência e da possibilidade de acesso a conexões de outros usuários, caso não hajam regras de proteção específica.

Dessa forma, como complementa Nakamura e Geus (2002), o enfoque muda de "impedir o acesso" para "controlar os usuários que acessam a rede". De fato, trafegar informações sigilosas em redes públicas, sem a devida segurança, pode resultar em prejuízos não mensuráveis. Para tanto, as VPN's lidam com conceitos fundamentais de segurança de criptografia e tunelamento que, embora não sejam focos deste presente trabalho, ao menos devem ser citados.

Contudo, pode-se afirmar que não é um produto que vai garantir a segurança necessária, mas sim a política de segurança definida e sua correta implementação. O melhor produto para a organização é aquele que melhor permite a implementação da política de segurança definida e que melhor se ajuste à experiência e capacidade dos profissionais.

5. Conclusão

Sob o cenário de economia globalizada, a incessante busca de inovações deve ser permanentemente valorizada, como afirma Amato (2000), não somente no que diz respeito às inovações de produtos, serviços e processos, mas também às novas formas de organização intra e interorganizacional, que exigem novos modelos administrativos.

Neste contexto, pode-se afirmar que as novas oportunidades de negócio tendem a privilegiar produtos e serviços que envolvem alto conteúdo de conhecimentos e de informações. Em decorrência disso, a emergência das redes de cooperação, manifestadas em suas diversas formas (consórcios, *clusters*, organizações virtuais, incubadoras de empresas e parques tecnológicos) ganham destaque especial e, além disso, apresentam-se como tendência universal e irreversível que tem possibilitado às PME's suprirem suas necessidades, além de lhes proporcionar benefícios competitivos.

A formação e desenvolvimento de redes de cooperação é uma grande oportunidade para que as PME's sejam fortalecidas, bem como sobreviverem frente às grandes empresas. Porém, apesar de todos benefícios acarretados pela formação das redes de cooperação, não se pode deixar de relevar os obstáculos, uma vez que as mesmas encontram-se em fase de implantação no Brasil e nem sempre bem sucedidas. Essas barreiras podem ser observadas em fatores como atividades redundantes, instabilidade e ausência de confiança entre os parceiros da rede.

De acordo com Bremer (2000), as tecnologias de informação e comunicação (como *Internet* e *Intranet*, tecnologia VPN, videoconferência e compartilhamento de arquivos), trazem consigo conseqüências extremamente relevantes no contexto empresarial e pode ser notada uma relação uma relação muito forte entre essas tecnologias e o avanço das cooperações entre empresas. Dessa forma, cabe às redes optarem pelo meio de comunicação e informação que melhor se adaptar à sua realidade financeira.

No entanto, como afirmam Nieto *et al* (2002), as empresas devem ter como preocupação primordial a segurança das informações trafegadas pela rede, pois as mesmas podem ser interceptadas por usuários não autorizados. A egurança em ambientes cooperativos será, então, o resultado do conjunto de esforços para entender o ambiente e as tecnologias, saber como utilizá-la e implementá-la de modo correto.

Diante do exposto, há necessidade de, primeiramente, diagnosticar quais os riscos aos quais a organização pode se expor para, a partir disso, poder analisar quais mecanismos de segurança se encaixam melhor à necessidade avaliada. Neste caso, vale ressaltar que, mesmo com os mecanismos de segurança, é difícil lidar com a complexidade gerada dos diferentes níveis de acesso existentes, sem comprometer a segurança bem como seus integrantes, pois quando várias conexões passam a se interligar, torna-se maior o risco de interferência e da possibilidade de acesso a conexões de outros usuários, caso não haja regras de proteção especificada.

Portanto, o enfoque passa a ser o de controlar os usuários que acessam a rede através da utilização concomitante dos mecanismos de segurança de criptografia e tunelamento de dados, para tratamento do ciframento e encapsulamento das informações, bem como o *firewall* para gerenciamento do tráfego dessas informações na rede .

Por fim, outros aspectos também primordiais estão relacionados à política individualista e visão de curto prazo, bem como a fatores comportamentais como a cultura empresarial, que impedem o desenvolvimento dessa nova estratégia organizacional de redes cooperativas. Conseqüentemente, essas empresas acabam perdendo seu mercado consumidor, pois os clientes tendem a serem cada vez mais exigentes, acarretando, geralmente, o fechamento de seu negócio, já que elas não têm condições de concorrer, sozinhas, com as grandes empresas.

Referências

ALBERTIN, A. L. *Comércio Eletrônico: seus aspectos de segurança e privacidade.* Revista Administração. Versão 38, nº 2, p. 49 – 61, 1998.

AMATO NETO, J. *Redes de Cooperação Produtiva e Clusters Regionais.* São Paulo: Atlas, 2000.

BREMER, C. F. *Redes de Cooperação.* Revista: Produtos e Serviços: Fábrica do Futuro – entenda hoje como vai ser sua indústria amanhã. Edição Especial, p 99 – 104. Dezembro 2000.

CARRETTO, B. A. *Formação de Redes de Cooperação entre Empresas: identificação das variáveis do paradigma cooperação/competição.* Dissertação de Mestrado – Escola de Engenharia de São Carlos – USP, 2002.

CASARROTO FILHO, N.; PIRES, H. L. *Redes de Pequenas e Médias Empresas e Desenvolvimento Local.* 2ª edição. São Paulo: Atlas, 2001.

GUTTMAN, D. J.; HERZOG, L. A. *Rigorous Automated Network Security Management.* International Journal of Information Security. Volume 4, n° 1 – 2, p. 29 – 48, fevereiro 2005.

LEON, E. M.; AMATO NETO, J. *Redes de Cooperação Produtiva: Uma Estratégia de Competitividade e Sobrevivência para Pequenas e Médias Empresas.* I Workshop: Redes de Cooperação e Gestão do Conhecimento. PRO-EPUSP, outubro 2001 – endereço: www.prd.usp.br/redecop/textos.htm (08/02/2003).

MEADOWS, A. J. *Knowledge and Communication: essays the information chain.* London: Library Association Publishing, 1991.

MUNDIM, F. P.A. *Proposta de um ambiente cooperativo suportado por computador para a participação de PME's em organizações virtuais.* Dissertação de Mestrado - Escola de Engenharia de São Carlos – USP, 1999.

NAKAMURA, T. E.; GEUS, L. P. *Segurança de Redes em Ambientes Cooperativos.* São Paulo: Berkeley, 2002

NEVES, F. V. F. *Uma Análise da Aplicabilidade do DataWarehouse no Comércio Eletrônico, Enfatizando o CRM Analítico.* Dissertação de Mestrado – Escola de Engenharia de São Carlos – USP, 2001.

NIETO, G. M. J.; BOYD, C. V.; DAWSON, E. C. A. *Key Recovery for the Commercial Environment.* International Journal of Information Security. Volume 1, n° 3, p. 161 – 174, novembro 2002.

PIGNATARI, D. *Informação, Linguagem, Comunicação.* 4ª edição. São Paulo: Perspectiva, 1970.

SANTOS, M. E.; REZENDE, O. S. *Tecnologia da Informação.* Revista: Produtos e Serviços: Fábrica do Futuro – entenda hoje como vai ser sua indústria amanhã. Edição Especial, dezembro 2000.

SOLMS, V. B.; SOLMSª, V. R. *From Information Security to Business Security.* Computers & Security. Volume 24, P. 271 – 273, 2005.

WURMAN, S. R. *Ansiedade de informação – como transformar informação em compreensão.* 5ª edição. Cultura Editores Associados,1995.