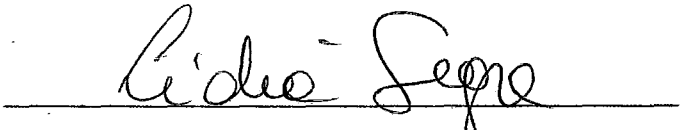
ESTRATÉGIAS EMPRESARIAIS NO MERCADO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASOS NO RIO DE JANEIRO

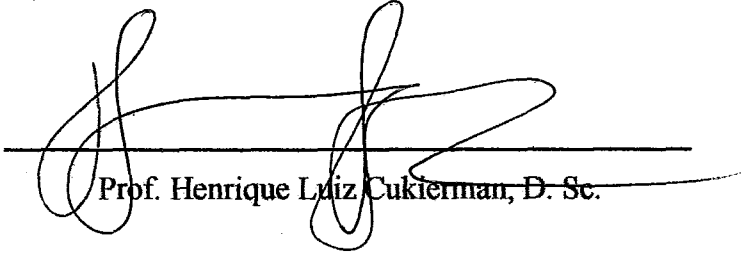
Bruno de Paula Ribeiro

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

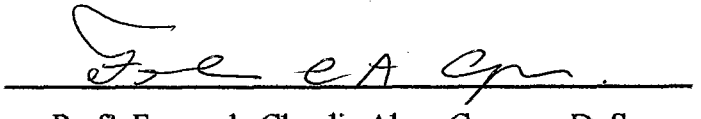
Aprovada por:



Profª Lidia Micaela Segre, D. Sc.



Prof. Henrique Luiz Cukierman, D. Sc.



Profª. Fernanda Claudia Alves Campos, D. Sc.

Prof. Ivan da Costa Marques, PhD.

RIO DE JANEIRO, RJ – BRASIL

MARÇO DE 2004

RIBEIRO, BRUNO DE PAULA

Estratégias Empresariais no Mercado Brasileiro de Segurança da Informação: Um Estudo de Casos no Rio de Janeiro [Rio de Janeiro] 2004

XII, 162 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2004)

Tese – Universidade Federal do Rio de Janeiro, COPPE

1. Mercado de Segurança da Informação no Brasil.

2. Estratégias competitivas para empresas de Segurança da Informação.

I. COPPE/UFRJ II. Título (série)

Dedico este presente trabalho a meus pais Dirceu e Sonia, pelo incentivo e suporte em todos os momentos da jornada.

Março de 2004.

Agradecimentos

À professora Lídia Segre, pelo trabalho de orientação neste estudo e paciência com os alunos, mesmo nos momentos mais difíceis e de agenda cheia.

Aos professores Henrique, Fernanda e Ivan, por sua participação na banca de avaliação.

Aos diretores e demais funcionários das empresas que serviram de estudo de caso, por sua disponibilidade de tempo, pelo seu interesse em tornar esta pesquisa possível e por acreditarem no potencial da tecnologia brasileira.

À minha irmã Stela, pela paciência comigo nos momentos mais difíceis e por suportar a quantidade de papel espalhada pela casa.

A todos os professores da COPPE e NCE, os quais me permitiram ter contato com áreas de conhecimento que só um curso de pós-graduação pode permitir.

Aos funcionários da COPPE, que sempre procuraram resolver os problemas burocráticos da melhor forma possível.

A Johanna Gavilanes e Maria Gardeborg pela revisão do resumo em inglês.

Às empresas onde trabalhei, por cederem o tempo necessário para a conclusão dos estudos, sem exigirem retorno.

E a todos os que, embora não citados, contribuíram de alguma forma para tornar este trabalho uma realidade.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M. Sc.)

ESTRATÉGIAS EMPRESARIAIS NO MERCADO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASOS NO RIO DE JANEIRO

Bruno de Paula Ribeiro

Março/2004

Orientadora: Lídia Micaela Segre
Programa: Engenharia de Sistemas e Computação

Em uma época de globalização e importância cada vez maior do conhecimento e das redes na economia dos países, a Tecnologia da Informação torna-se uma peça chave para o desenvolvimento de qualquer nação. Neste contexto, têm surgido preocupações relativas à segurança eletrônica para empresas, governos, instituições financeiras e demais organizações. Tais preocupações motivaram a criação de um novo mercado, onde empresas especializadas prestam serviços e desenvolvem produtos voltados para a segurança. Este mercado ainda é bastante novo e encontra-se em definição, mas se apresenta como promissor em vários países. O objetivo deste trabalho é analisar os conceitos relacionados à Segurança da Informação, os mecanismos associados, o mercado deste segmento, as empresas relacionadas e as estratégias competitivas empregadas, a partir de uma revisão bibliográfica nacional e internacional e de um estudo de casos realizado em três firmas nacionais de segurança. Dentre os principais resultados, identificamos algumas tendências para o setor, com foco nas atividades de desenvolvimento de *software* de segurança. Também identificamos alguns aspectos importantes a serem levados em consideração por políticas governamentais para a área de segurança e outros que possam ser úteis para o empreendedor brasileiro de TI, na sua jornada contínua de tomada de decisões e elaboração de estratégias.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

MANAGEMENT STRATEGIES IN BRAZILIAN INFORMATION SECURITY MARKET: CASE STUDIES IN RIO DE JANEIRO

Bruno de Paula Ribeiro

March/2004

Advisor: Lídia Micaela Segre

Department: Systems and Computer Engineering

At days of globalization and increasing of the importance of knowledge and networks for worldwide economy, the IT industry arises as a key piece for the development of any nation. In this context, IT security concerns arise for enterprises, public administrations, financial companies and other organizations. Such concerns have caused the creation of a new market, where expert companies offer services and products developed for electronic security. This is a business under definition, still very young, but with a very promising future in many countries. The purpose of this work is to analyze the concepts related to the Information Security field, its technologies, market/players, and competitive strategies used, starting from a theoretical approach both national and international, and case studies promoted with three Brazilian e-security companies. Among the main results, we identified some tendencies for this market, with focus on security software development. We also identified some important aspects that should be considered in government policies for the security field, and other factors that may be useful for Brazilian technology entrepreneurs along their continuous journey in decision making.

ÍNDICE DO TEXTO

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1 INTRODUÇÃO

As últimas duas décadas, em especial a década de 1990, mostraram ao mundo a importância da Tecnologia da Informação (TI) para a sociedade como um todo, principalmente contextualizando essa revolução tecnológica no ambiente da globalização mundial. Mais importante ainda é o impacto dessas tecnologias na economia dos países, que pode ser observado na independência tecnológica do país, na geração de empregos e no maior fluxo financeiro. Como resultado da maior disseminação da TI, surgiu também a chamada Nova Economia, termo utilizado para se referir ao contexto econômico atual, baseado em uma importância cada vez maior do conhecimento.

Sem a intenção de fazer aqui um histórico da evolução da tecnologia de informática em todo mundo, não podemos fugir de analisar os passos que levaram a computação ao grau onde ela está hoje, de forma a compreender as recentes necessidades por segurança, segmento da TI que nos interessa neste estudo. E isto abrange essencialmente temas tais como arquitetura cliente/servidor, redes de computadores e *downsizing*.

Houve um aumento significativo da capacidade dos microcomputadores nos últimos 20 anos, os quais foram gradativamente tomando o lugar dos computadores de grande porte em várias empresas. A arquitetura cliente/servidor, galgada em microcomputadores, vem há um bom tempo substituindo, de maneira revolucionária, a tradicional computação baseada em *mainframes* e processamento em lote.

A essa revolução do *hardware*, somou-se a sofisticação dos sistemas operacionais e dos *softwares*, permitindo uma maior integração em rede e uma automação dos processos empresariais. Como cita Castells (1999, p. 62):

> Desde meados da década de 1980, os microcomputadores não podem ser concebidos isoladamente: eles atuam em rede, com mobilidade cada vez maior, com base em computadores portáteis. Essa versatilidade extraordinária e a possibilidade de aumentar a memória e os recursos de processamento, ao compartilhar a capacidade computacional de uma rede eletrônica, mudaram decisivamente a era dos computadores nos anos 1990, ao transformar o processamento e armazenamento de dados centralizados em um sistema compartilhado e interativo de computadores em rede.

A partir de meados da década de 1990, o mercado mundial de Tecnologia da Informação sofreu uma mudança revolucionária, impulsionada pelas redes de trocas de dados, em especial a Internet. As redes já vinham sendo largamente utilizadas nas grandes empresas, facilitando a comunicação dos funcionários, interligando filiais e automatizando processos da organização. Entretanto muitas empresas menores ainda podiam se dar ao luxo de não utilizarem as tecnologias de rede. Algumas empresas sequer utilizavam computadores no seu dia-a-dia.

Com a chegada da Internet, várias organizações se sentiram tentadas a estender seus negócios para a *Web*, mesmo sem saber ao certo o propósito disto. Surgiram as empresas "ponto com", ou seja, aquelas baseadas integralmente na Internet (várias delas sem um escritório físico determinado). Negócios passaram a ser feitos através das redes, e a maioria das empresas passou a disponibilizar seus serviços aos clientes pela *Web*.

O processo foi ocorrendo em uma velocidade jamais vista, fazendo com que empresas e pessoas fossem pegas de surpresa. Na mesma velocidade, também chegaram as questões de segurança, relacionadas a esse novo contexto. Como as tecnologias de redes de computadores não haviam sido planejadas para trocas comerciais e negócios em geral, elas naturalmente não contavam com mecanismos adequados de segurança. Em pouco tempo, os prejuízos para as empresas começaram a ser manchete de jornal, junto com os vilões causadores dos mesmos: os *hackers*.

De acordo com Tanembaum (1997), durante as duas primeiras décadas de existência das redes de computadores, o seu uso estava restrito a pesquisadores universitários, que basicamente enviavam *e-mails*, e a funcionários de empresas, que precisavam compartilhar impressoras. Neste contexto, a segurança não tinha praticamente a menor importância. Mas hoje em dia, milhões de pessoas utilizam as redes para realizar operações bancárias, compras, declaração de imposto de renda, dentre outras atividades, de forma que a segurança passa a ser um problema em potencial.

O quadro atual aponta para uma maior dependência da sociedade com as Tecnologias da Informação. Yourdon (2002) observa que estaremos vendo uma integração dos bancos de dados dos setores público e privado em todo o mundo, o que aumentará a importância de questões de segurança, como a privacidade. Conseqüentemente iremos presenciar um enorme aumento nas técnicas e tecnologias para a proteção das redes de telecomunicações, dos *sites*, dos portais de Internet e de outros aspectos dependentes da tecnologia dos computadores.

Essa maior dependência da sociedade com os computadores torna o problema da segurança muito mais complexo, tirando o mesmo apenas do âmbito puramente tecnológico. Nas palavras de Yourdon (2002, p. 8):

> Em alguns casos, o ataque pode não ser feito no computador *per se*, mas na habilidade dos sistemas de computadores de suportar funções críticas tais como centrais telefônicas, sistemas de transações financeiras, controle de tráfego aéreo, etc.

Os acontecimentos mais recentes nas nações líderes do capitalismo estão sendo responsáveis por um deslocamento de preocupações no que diz respeito às tecnologias. É o caso dos atentados terroristas de 11 de setembro, nos Estados Unidos, que provocaram uma queda econômica exacerbada em muitas companhias, e já estão causando uma mudança de foco de atuação em direção ao mercado militar, governamental e de atividades de computação relacionadas à segurança.

Segundo Yourdon (2002), a forma como os dólares associados aos custos com TI serão gastos irá provavelmente mudar de maneira significativa, sendo um percentual muito maior dedicado à segurança, recuperação de desastres e planejamento de contingência.

É nesse contexto que problemas de segurança se apresentam para o mundo, e, na tentativa de propor soluções de toda ordem para eles, surge um novo mercado: o de Segurança da Informação. Entretanto este mercado ainda é muito novo, pouco definido e difundido.

Por esses fatores, consideramos a Segurança da Informação como um segmento bastante promissor para o desenvolvimento da indústria de TI no Brasil, em especial a indústria de *software*. Em nossa opinião, o país precisa participar da economia mundial, e não apenas como um simples comprador de tecnologia. A indústria de TI é uma das mais importantes no mundo, pois não consome recursos naturais, traz retornos financeiros altíssimos e desenvolve uma mão-de-obra extremamente qualificada, dentre outros fatores.

Partimos do pressuposto que o quadro atual é bastante desfavorável ao Brasil, em se tratando da competição global do mercado de TI. Apesar do sucesso na produção de *hardware* nos anos 1970 e 1980 e do potencial de desenvolvimento de *software* existente no país, é possível ver que o mercado brasileiro está cada vez mais dominado por empresas estrangeiras, e as poucas companhias nacionais sobrevivem em meio a todo tipo de adversidade. O pequeno e médio empreendedor de tecnologia, que deveria

ser a base do desenvolvimento de nossa economia nesta área, assim como ocorre nos países desenvolvidos, está abandonado à mercê do mercado e em uma busca desesperada por investimentos de capital estrangeiro. Empresas que chegaram a despontar em todo o país e até a ousar aparecer no exterior, atualmente vivem crises financeiras, acentuadas pelas crises mundiais que se iniciaram no final do século XX. A agenda das empresas passou de expansão de mercados para sobrevivência.

Neste estudo, optamos por analisar o segmento de Segurança da Informação pelas seguintes razões: (i) trata-se de uma área bastante recente, que ainda não está totalmente definida no Brasil nem em outros países, representando, dessa forma, uma chance importante para entrarmos no mercado global de tecnologia; (ii) as principais tecnologias de segurança estão baseadas em *software*, uma área para a qual, na nossa visão, o Brasil possui capital humano e potencial para exportação; (iii) a segurança está diretamente ligada com a Internet e as recentes preocupações mundiais, como o terrorismo.

Segundo Yourdon, os atentados de 11 de setembro de 2001 provocaram uma mudança de paradigma na Tecnologia da Informação, como ele coloca a seguir:

> Se os ataques de 11 de setembro tivessem ocorrido em 1974, o primeiro ano em que o *World Trade Center* abria para negócios, então a maioria dos cidadãos esperaria desempenhar um papel passivo em qualquer discussão relacionada a conseqüências na área de TI. Mas, hoje em dia, o cidadão médio possui mais poder computacional em seu computador pessoal do que todo o campus do MIT em 1974 (YOURDON, 2002, p. 14).

A experiência de seis anos do autor deste trabalho na área de Segurança da Informação também motivou a escolha por esse campo de estudo. Mas, principalmente, a vivência com outras pessoas da linha de pesquisa Informática e Sociedade, do Programa de Engenharia de Sistemas e Computação da COPPE/UFRJ, e, acima de tudo, as disciplinas estudadas no curso de Mestrado, envolvendo questões como o impacto das tecnologias na sociedade e na economia do país, foram fatores determinantes na decisão por pesquisar estes temas interdisciplinares.

A partir das idéias acima, listamos os seguintes objetivos para este estudo:

- Analisar os conceitos relacionados ao campo da Segurança da Informação, assim como o mercado para a área, as empresas nacionais e internacionais e suas formas de atuação.

- Analisar as condições em que empresas brasileiras da área de segurança estão operando, e levantar barreiras e necessidades, verificando as principais estratégias de gestão que estão sendo adotadas por seus executivos.
- Identificar aspectos importantes a serem incluídos em políticas governamentais para o fomento de empresas nacionais de Segurança da Informação.

No decorrer do estudo, mostramos a importância da indústria de *software* para o setor de TI brasileiro, e que as principais empresas de Segurança da Informação no mundo são justamente as que investiram seus esforços de Pesquisa e Desenvolvimento em tecnologias de *software*.

Damos uma ênfase às estratégias competitivas para a Nova Economia, embasadas na gestão do conhecimento e da inovação. Isto se deve ao fato de que tais estratégias precisam ser levadas em conta por empresas que lidam com tecnologia de ponta, antes que seja tarde, nas condições atuais resultantes do processo de globalização. Como destaca Passos (1999, p.64):

> Sistemas de gestão [...] não podem ser implementados repentinamente, apenas quando a concorrência se fizer presente e aguda. Nesse momento talvez já seja tarde demais para a sua sobrevivência.

Como resultados e contribuições, pretendemos identificar as principais tendências para o setor de Segurança da Informação, as dificuldades que os empresários da área vêm enfrentando e apresentar as suas experiências, de forma que possam ser úteis a outros empreendedores do mesmo ramo. Também levantamos alguns pontos a serem considerados pelos formuladores de políticas para área de Tecnologia da Informação, em especial de segurança, no Brasil, com a esperança de vê-los refletidos no futuro.

1.1 Metodologia

A fundamentação teórica deste estudo foi realizada através de uma revisão bibliográfica sobre a Tecnologia da Informação, com foco na indústria de *software*, sobre as estratégias empresariais para empresas de TI e sobre a área de Segurança da Informação, em particular no Brasil, com base em livros e periódicos nacionais e internacionais. Foram pesquisadas ainda teses e *sites* na Internet sobre os temas mencionados. A novidade do tema Segurança da Informação, ainda não totalmente estabelecido e coberto por estudos acadêmicos, fez com que a maior parte das

informações sobre este assunto tivesse que ser obtida através de dados disponíveis na mídia especializada.

Para a verificação das informações obtidas na revisão teórica, realizamos um estudo de casos em três empresas que atuam na área de Segurança da Informação, na cidade do Rio de Janeiro. Pelo fato deste mercado ainda ser bastante novo, existem poucas empresas que podem ser consideradas da área de segurança, de forma que o critério para a escolha dessas empresas foi bastante simples. Basicamente, foram selecionadas as empresas cariocas que mais aparecem nos meios de comunicação brasileiros voltados para a área de segurança. Após uma rápida pesquisa na Internet e conversa com especialistas da área, foi possível perceber que as três empresas escolhidas são as únicas, na cidade do Rio de Janeiro, a possuírem uma história na área de segurança e uma experiência de aplicação dos serviços mais conhecidos deste segmento. Uma outra empresa carioca, que ficou fora do estudo, nunca possuiu competência na área de desenvolvimento de *software*, algo que foi considerado de suma importância para a análise. Outras empresas existentes são apenas consultorias na área de redes ou Internet, que apresentam em seus *sites* corporativos a oferta de serviços de segurança, e por isso não se aplicavam aos estudos de casos.

Para analisar as empresas selecionadas, foram utilizadas duas fontes de informação. A primeira foi a vivência do autor, já que o mesmo trabalhou em duas das empresas e com os sócios da terceira, durante um período total de seis anos. Nesta vivência, foi possível aprofundar informações sobre segurança, gestão empresarial e desenvolvimento de *software*, além de estabelecer um contato muito estreito com funcionários, gerentes e sócio-diretores. Este contato poderia ser visto como um ponto negativo para a imparcialidade do estudo, entretanto ele ocorreu com as três empresas de forma equivalente, além de que o autor sempre atuou na área técnica, sendo um observador dos processos de gestão das companhias.

A segunda fonte de informações foi a realização de entrevistas pessoais, por *e-mail* e telefone, com base em um questionário (apresentado no Anexo II) direcionador das conversas e de outras questões que foram surgindo até a conclusão do trabalho. Todas as entrevistas foram realizadas com pessoas de cargos de diretoria ou gerência nas empresas, de preferência sócio-fundadores, sendo que foram ouvidas no mínimo duas pessoas para cada estudo de caso. As entrevistas foram gravadas em fita cassete e transcritas após a realização. Estas transcrições não fazem parte desse texto, e serviram apenas como base para a elaboração dos estudos de caso.

1.2 Organização do texto

A seguir apresentamos a estrutura da presente dissertação, que consta de sete capítulos, incluindo esta introdução.

O capítulo 2 apresenta as necessidades e os problemas de segurança relacionados aos segmentos específicos da TI. Em particular, focalizamos as redes de computadores inseridas do ambiente corporativo e as mais modernas aplicações da Internet, como o Comércio Eletrônico. Também é analisado o impacto das questões de segurança em dois setores da economia que são de extrema importância: o governamental e o financeiro, considerados os mais interessados em Segurança da Informação.

No capítulo 3, fazemos uma revisão dos principais aspectos relacionados à Tecnologia da Informação no Brasil, com foco na área de *software*, incluindo a posição do país na economia globalizada, a disponibilidade local de recursos para a indústria de Informática e as políticas que já foram implementadas no país com o intuito de alavancar o setor. Apresentamos uma classificação proposta pela Sociedade SOFTEX (2002) para o modelo de negócios das empresas de *software*, e uma pesquisa realizada pela coordenação geral da organização, que traz informações a respeito da situação atual dessa indústria no país.

O capítulo 4 apresenta uma revisão teórica sobre as principais estratégias empresariais recomendadas para as empresas da Nova Economia, de acordo com autores nacionais especializados no assunto, com foco no Brasil e nas firmas de TI. São tratadas questões como a importância do conhecimento, a aprendizagem organizacional e as estratégias competitivas. Utilizamos dois modelos propostos por Fleury e Fleury (1999), um para a classificação das estratégias e outro para o posicionamento global das empresas. São focalizadas as estratégias nas pequenas e médias empresas (PMEs) e a importância do relacionamento entre elas, fator que trouxe sucesso a diversos países ao redor do mundo.

O capítulo 5 introduz o leitor, de uma maneira genérica, no universo da Segurança da Informação e das empresas que atuam neste nicho de mercado. São discutidos os principais conceitos teóricos da segurança e os principais tipos de produtos e serviços operados pelas empresas. Apresentamos uma análise sobre o mercado de segurança no mundo e as suas companhias mais influentes e bem sucedidas, as quais, em sua maioria, investiram bastante em tecnologias de *software*. Finalmente, destacamos algumas tendências para o setor, de acordo com especialistas da área.

O capítulo 6 apresenta a descrição dos três estudos de caso escolhidos, focados nos principais tópicos da revisão teórica. Realizamos uma análise comparativa dos resultados obtidos, destacando principalmente a caracterização das empresas nos modelos adotados para o desenvolvimento de *software*, a estratégia empresarial utilizada, o posicionamento competitivo global e o tipo de atuação no mercado de segurança.

Finalmente no capítulo 7, são apresentadas as conclusões do estudo e uma análise geral dos resultados obtidos com os estudos de caso. Aproveitamos para sugerir alguns aspectos importantes que poderiam ser considerados em políticas de fomento para empresas nacionais de segurança, com um foco especial para o desenvolvimento de *software*. Propomos ainda alguns temas para trabalhos futuros, que poderiam dar continuidade a este estudo.

Além dos capítulos já descritos, este texto possui no final a lista das referências bibliográficas utilizadas e uma sessão de anexos, contendo um glossário de termos incomuns e o guia de entrevistas utilizado nos estudos de caso.

2 A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

> Mas a maioria dos livros recentes que tratam do futuro dos computadores e do campo da Tecnologia da Informação (TI) tem focado em um futuro glamuroso para o *e-commerce* e a Internet; ironicamente, este futuro parece muito menos glamuroso do que foi há bem pouco tempo atrás (YOURDON, 2002, p. xiii).

Neste capítulo, iremos tratar da importância da Segurança da Informação para quatro importantes atores no mercado de Tecnologia da Informação:

- Redes corporativas;
- Comércio Eletrônico;
- Instituições governamentais;
- Instituições financeiras.

É importante notar que estes diferentes atores, no fundo, possuem interligações e áreas de intersecção. Tal subdivisão foi adotada apenas para facilitar o levantamento das necessidades de segurança.

2.1 Segurança da Informação no mercado das redes corporativas

As redes de computadores estão intrinsecamente ligadas com as questões de segurança. Pode-se até dizer que toda a grande preocupação com segurança eletrônica surgiu graças ao advento das redes, o que tornou o problema mais intenso e complexo. Além disso, não é de se estranhar que os profissionais pioneiros no campo da Segurança da Informação tenham vindo da área de redes. O impacto das redes no mundo da tecnologia é tão grande, que atualmente não podemos mais conceber a idéia de informática sem pensar nelas.

Tanembaum (1997) observa que há 20 anos atrás, uma empresa de médio porte ou uma universidade contava com apenas um ou dois computadores, e as grandes instituições tinham, no máximo, algumas dezenas de máquinas. Com o passar do tempo, os computadores foram diminuindo de tamanho e de preço, e ganhando importância no meio corporativo. A fusão dos computadores com as telecomunicações teve uma profunda influência na organização dos sistemas computacionais, deixando para a

história o conceito de Centro de Processamento de Dados (CPDs). Entravam em cena as chamadas redes de computadores.

Ao se falar em "redes corporativas", subentende-se toda a infra-estrutura de suporte a interconexão de computadores dentro de uma instituição empresarial[1], que envolve as estações de trabalho, os servidores, o cabeamento estruturado, os roteadores, os *firewalls*, os sistemas operacionais de rede, os *softwares* de administração e suporte a redes, etc. A demanda por produtos (*hardware* e *software*) de redes aumentou consideravelmente com o advento da arquitetura cliente/servidor (citada na introdução deste capítulo), que substituiu na grande maioria das empresas os antigos sistemas de *mainframe*. Fora isso, novos profissionais de computação entraram em cena, os administradores de rede, e, com estes, toda uma equipe de suporte portadora de conhecimentos bastante especializados no assunto.

Discutiremos a seguir os principais aspectos das redes corporativas.

2.1.1 Histórico

A história das redes de computadores remonta aos anos 1970. Segundo Tanembaum (1997), a motivação para o desenvolvimento destas redes foi a necessidade de extrair e correlacionar informações sobre toda uma instituição, já possuidora de computadores, porém desconectados.

Naquela década, os importantes avanços nas áreas de tecnologia de telecomunicações e de integração de computadores em redes foram importantes fatores para a viabilização das redes. Foi um período de grande avanço científico: desenvolveram-se os roteadores e comutadores eletrônicos e as tecnologias de transmissão, responsáveis por implementar o conceito de nós de uma rede de computadores. Mas tais avanços só foram possíveis graças à evolução da microcomputação digital, que também avançou bastante na mesma década.

Um divisor tecnológico, como diz Castells (1999), para as redes de computadores, ocorreu justamente no ano de 1970, com a instalação de uma nova e revolucionária rede eletrônica de comunicação pela ARPA, a qual se desenvolveu durante toda a década e veio a se tornar a Internet de hoje.

---

[1] É claro que as redes também são usadas em instituições governamentais, universidades, bancos e demais organizações. Mas o enfoque aqui é dado às empresas, públicas ou privadas, que foram as primeiras a enfrentar as mudanças organizacionais significativas introduzidas pelas redes.

Somente na década de 1990 é que as empresas foram perceber o extraordinário potencial da Internet. A partir daí, as redes corporativas passaram a se conectar à rede mundial de computadores, possibilitando a seus funcionários um acesso maior e mais rápido às informações, através de serviços como, por exemplo, *e-mail, browser e* FTP. Os sistemas então se sofisticaram a ponto de cada empresa possuir a sua própria Internet privada, a *Intranet*, oferecendo aos empregados da companhia todas as informações, que antes estavam disponíveis apenas nos servidores de rede, através de uma linguagem e formato comuns: a linguagem da Internet.

Atualmente as redes fazem parte de qualquer grande sistema computacional, seja em empresas, universidades, institutos de pesquisa, e até mesmo nas casas das populações mais desenvolvidas em todo o mundo, através da Internet. A geração dos anos 1990 não conhece o conceito de informática separado das redes. E é provável que a geração atual o desconheça dissociado da Internet.

2.1.2 Vantagens

As redes se disseminaram rapidamente no meio corporativo por uma série de vantagens, quase todas ligadas ao compartilhamento de recursos e à correlação de informações.

Tanembaum (1997) cita algumas vantagens trazidas para as empresas pelas redes de computadores:

- Compartilhamento de recursos: conceito chave das redes. Os recursos compartilhados podem ser, por exemplo, programas, equipamentos e, especialmente, dados;
- Aumento da confiabilidade dos sistemas: com as redes, ficam disponíveis fontes alternativas de fornecimento de recursos. Esta disponibilidade é essencial em operações militares, financeiras, de controle de tráfego aéreo e na segurança de reatores nucleares, por exemplo;
- Economia de dinheiro: com a arquitetura cliente/servidor, é possível trocar os imensos e caros *mainframes* por máquinas servidoras e estações de trabalho extremamente mais baratas;
- Escalabilidade: as redes possibilitam que uma empresa aumente gradualmente o desempenho de seus sistemas de informação, à medida que cresce o volume de carga, bastando para isso a adição de novos computadores;

- Meio de comunicação eficaz: as redes podem oferecer aos funcionários das empresas uma forma singular de comunicação e interação, podendo aqueles estar em locais bem distantes um dos outros.

O ganho em produtividade que as companhias obtiveram com as redes foi bastante motivador, principalmente em uma época em que os recursos computacionais eram proibitivamente caros. Este ganho de produtividade veio através do compartilhamento de recursos e da propagação da informação.

Atualmente não se fala mais em vantagens trazidas pelas redes, já que as mesmas fazem parte inseparável dos sistemas de informação de qualquer instituição em todo o mundo.

2.1.3 Mudança Organizacional

As redes de computadores trouxeram não apenas tecnologia para as empresas, mas também promoveram uma mudança significativa na estrutura organizacional das mesmas.

Segundo Castells (1999), o avanço tecnológico das redes permitiu o surgimento de processos flexíveis e interativos na cadeia produtiva (gerenciamento, produção e distribuição), envolvendo uma cooperação maior entre empresas, suas unidades, fornecedores e clientes. Dessa forma, as redes contribuíram para uma certa crise, ou na maioria das vezes, uma reestruturação na organização das antigas e grandes empresas verticais[2].

Mas ao mesmo tempo em que a tecnologia de redes motivou mudanças organizacionais, estas também definiram em grande parte os destinos da própria tecnologia. A organização em rede faz parte da nova configuração da economia global, da teia de empresas e alianças estratégicas, das subcontratações e do relacionamento com clientes. Pode-se dizer que toda essa configuração seria praticamente impossível sem as redes de computadores e as estações de trabalho com microcomputadores poderosos. Como diz Castells (1999), este é um caso em que a transformação organizacional (descentralização), de certa forma, motivou a trajetória tecnológica. É provável que se as grandes empresas verticais tivessem sido capazes de continuar a operar com sucesso na Nova Economia, a crise dos *mainframes* não teria ocorrido.

---

[2] Termo utilizado para se referir às organizações baseadas em grandes hierarquias e organogramas rígidos. Já as empresas horizontais, ao contrário, são baseadas em processos mais flexíveis.

As redes também capacitaram as empresas a gerir melhor a informação e a focar seus esforços nas suas competências essenciais, através de estratégias de terceirização e mudanças na estrutura da organização como um todo.

2.1.4 Segurança

As redes de computadores, vitais para qualquer empresa do mercado atual, mesmo que de pequeno porte, como vimos nos itens anteriores, exigem que questões relativas à segurança sejam tomadas a sério pelas organizações, de uma maneira jamais ocorrida.

Os benefícios e vantagens das redes de computadores aqui apresentados vieram acompanhados de riscos. Com o acesso de funcionários à rede, através de todas as filiais, os recursos computacionais e as informações sigilosas podem então ser acessados por pessoas não autorizadas. Surge o primeiro problema básico da Segurança da Informação: o **controle de acesso**, que será visto no capítulo 5. Para agravar mais a situação, a partir dos anos 1990, as empresas passaram a conviver com um problema de segurança muito maior: a Internet.

Em termos técnicos, as redes de computadores estão originalmente baseadas em uma tecnologia insegura. De acordo com Puttini (2003), o protocolo IP[3] é muito simples, e exige apenas uma linguagem padrão de comunicação, permitindo a qualquer máquina enviar e receber pacotes na Internet, sem nenhuma autenticação ou criptografia. A Internet levou o problema do controle de acesso para fora da empresa, deixando as informações corporativas vulneráveis ao acesso indevido por pessoas externas à organização.

Tais preocupações aumentaram bastante com o advento dos ***hackers***. Mas atualmente, não apenas estes apresentam perigo para a "sociedade em rede", definida por Castells (1999). A complexidade da infra-estrutura de redes aumentou de tal forma que pequenos erros de planejamento, instalação e configuração podem resultar em desastres. A falha nas especificações de segurança ou no controle de acesso (ou até mesmo na completa ausência destes) em uma empresa pode ser explorada de diversas maneiras por indivíduos mal intencionados, dentro e fora da organização. O resultado

---

[3] O protocolo IP (*Internet Protocol*) é intrinsecamente inseguro por não conter, nem prever, a possibilidade de nenhum mecanismo de autenticação de nós ou de rota, sendo a autenticação um dos mecanismos básicos da segurança, como será visto no capítulo 5.

pode ser desde o constrangimento para a imagem da empresa até perdas financeiras catastróficas.

Os **vírus**, que já ameaçavam as empresas através da troca de disquetes entre pessoas, foram potencializados em sua disseminação com o advento das redes. Eles se espalham todos os dias, por toda a parte, provocando desde sustos e dores de cabeça a destruições completas de sistemas.

Os funcionários das companhias também passaram a apresentar ameaça, na medida em que precisam acessar a Internet para desempenhar suas funções. Com ou sem más intenções, estas pessoas podem servir de porta de entrada para inúmeros perigos.

Em outras palavras, a preocupação inicial com segurança trazida pelas redes de computadores ao ambiente corporativo evoluiu para um conceito muito maior de **segurança corporativa**, que envolve políticas, procedimentos e ações para proteger as informações sigilosas de uma empresa. Este é o mercado de segurança das redes corporativas, que vem sendo explorado por várias empresas em todo o mundo.

Os últimos anos têm mostrado um grande investimento em segurança por parte da maioria das empresas. A difusão das redes, a maior dependência de sistemas computacionais e os últimos acontecimentos do mundo têm feito com que o investimento em segurança corporativa deixasse de ser apenas um luxo, para se tornar uma necessidade vital.

Yourdon (2002) diz que uma das implicações estratégicas dos atentados terroristas de 11 de setembro será a noção de que as organizações terão de responder muito mais rapidamente aos ataques, uma vez que estes sejam percebidos. E lembra que foi um outro tipo de ameaça, o "*bug* do milênio", ou Y2K, que fez com que gerentes de TI, de negócios, administradores públicos e cidadãos comuns percebessem o quanto nossos negócios, nossos governos e nossa sociedade se tornaram dependentes de sistemas computacionais. Com o 11 de setembro, começamos a perceber o quão fatal pode ser esta dependência.

2.2 Segurança da Informação no mercado de Comércio Eletrônico

O termo *e-commerce* (ou Comércio Eletrônico), incorporado de forma praticamente obrigatória nas estratégias de *marketing* das empresas dos dias atuais, de uma maneira geral se refere ao comércio e aos negócios realizados pela Internet. Devido

a um excesso de especulação e exagerada expectativa, muitas empresas estimaram além do que se deveria as possibilidades da Internet, e chegaram a acreditar que o Comércio Eletrônico passaria a ser a única maneira de se fazer negócios em um futuro próximo.

Passada a euforia e a crise, que veio com a queda das ações das empresas "ponto com", hoje se entende que o Comércio Eletrônico funciona mais como um complemento aos negócios de uma empresa, usando a Internet como meio. Em casos mais específicos, o Comércio Eletrônico pode transformar completamente essa maneira de se fazer negócios. Mas não deve ser visto como atividade fim.

Quando compramos CDs, fazemos pedidos ao supermercado, nos inscrevemos em um curso, ou compramos um novo computador através da Internet, estamos participando do Comércio Eletrônico (neste caso em particular, conhecido como B2C, ou *Business to Client*). Atualmente, todas as grandes empresas estão disponibilizando a venda dos seus produtos e serviços pela *Web*, agilizando bastante o processo de entrega e tornando o produto mais barato, já que dessa forma eliminam-se os intermediários do processo de venda.

Vejamos alguns aspectos do Comércio Eletrônico a seguir.

2.2.1 Definições

Existe um número bastante grande de definições de Comércio Eletrônico. Neste trabalho, procurou-se reunir algumas definições dadas por autores especialistas na área.

Almeida (2000) coloca que o conceito de Comércio Eletrônico entrou para o vocabulário dos negócios durante as décadas de 1970/1980, quando estava então intimamente associado ao uso da tecnologia de EDI (*Electronic Data Interchange*).

O conceito de EDI é precursor ao de Comércio Eletrônico, e mais voltado para o que poderíamos chamar de *e-business*, ou negócios eletrônicos. EDI é a sigla em inglês para troca eletrônica de dados. A sua idéia básica é a da troca de mercadorias e serviços baseada em ligações eletrônicas entre os parceiros de negócio. Os sistemas de EDI mais famosos e antigos são os de reservas de passagens aéreas, de transferência de fundos entre bancos e sistemas de pedidos aos fornecedores na indústria automobilística (ALBERTIN, 1999).

A idéia principal do EDI está na padronização de mensagens, como uma espécie de protocolo para as comunicações entre sistemas de diferentes empresas. Através destas mensagens padronizadas, aplicações de *software* distintas, pertencentes a empresas também distintas, podem trocar transações de negócios entre si. Segundo

Almeida (2000), o EDI apenas especifica o formato da informação de negócio; a transmissão efetiva da informação é realizada por mecanismos de transporte como *e-mail* ou conexões ponto-a-ponto.

O EDI é tradicionalmente uma tecnologia cara, mais voltada para grandes empresas. Com as novas tecnologias da Internet, a utilização do EDI tende a aumentar, pois pequenas e médias empresas podem considerar viável a sua implantação. E é neste ponto que o EDI evolui para o *e-business*, em escala mundial.

Almeida (2000) traz duas definições importantes, uma para *e-business* e outra para *e-commerce*:

- *E-business* ou negócio eletrônico: jargão lançado por fornecedores como a IBM, que representa o conjunto de negócios eletrônicos possíveis a uma empresa, onde uma organização mantém uma relação comercial com parceiros, fornecedores, clientes e funcionários pela Internet.
- *E-commerce* ou Comércio Eletrônico: termo mais confuso, pois, para aqueles que consideram a definição de *e-business*, o *e-commerce* seria um de seus módulos, que representaria a troca de transações eletrônicas entre empresas distintas. Entretanto, o termo Comércio Eletrônico é conceituado de forma muito mais abrangente.

Essa forma mais abrangente, segundo a autora, se refere ao novo contexto da Internet, que acabou por criar uma série de siglas, uma para cada aplicação específica, tais como B2B (*Business to Business*), B2C (*Business to Client*), B2G (*Business to Government*) e G2G (*Government to Government*).

Uma definição genérica para o Comércio Eletrônico propriamente dito é apresentada por Albertin (1999, p. 15):

> O Comércio Eletrônico é a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos do negócio. Os processos podem ser realizados de forma completa ou parcial, incluindo as transações negócio-a-negócio, negócio-a-consumidor e intra-organizacional, numa infra-estrutura predominantemente pública de fácil e livre acesso e baixo custo.

Neste caso, o autor unifica todas as siglas citadas acima no conceito de processo de negócio. A questão central está no uso intenso de tecnologias de comunicação e informação. B2B, B2C, B2G ou G2G seriam diferentes processos de negócios.

No Comércio Eletrônico, as transações em papel são substituídas por transações eletrônicas (ALMEIDA, 2000). Quando se fala em transações, inclui-se também uma rede de publicidade eletrônica, com *homepages* altamente sofisticadas, *banners* em *sites* diversos e *e-mails* do tipo mala-direta, usando as mais modernas técnicas de *marketing*. Essa publicidade leva grande parte das pessoas a comprar determinados produtos, usando "dinheiro eletrônico" e outras formas de pagamento pela rede.

Neste trabalho, podemos simplesmente assumir que o Comércio Eletrônico corresponde à compra e venda de informações, produtos e serviços, seja entre empresas, governo ou cidadãos, através das redes de computadores.

O Brasil detém liderança na América Latina em *e-business* (40% do total) (SOCIEDADE SOFTEX, 2002). Entretanto, estima-se que apenas dez empresas sejam responsáveis por 80% do faturamento do mercado de *e-commerce* no país. No caso de B2C, o mercado brasileiro representa 60% do mercado latino-americano, com boas previsões de crescimento.

2.2.2 Mudança Organizacional

Assim como as redes de computadores, as tecnologias e processos relacionados com o Comércio Eletrônico vêm provocando mudanças na estrutura organizacional das empresas.

Almeida (2000) observa que a introdução de EDI torna as empresas totalmente dependentes dos sistemas automatizados, ao mesmo tempo em que aumenta a "interdependência" entre os parceiros envolvidos nas relações comerciais. Desta forma, a integridade do sistema passa a ser uma preocupação de todos os parceiros, pois erros podem ser propagados por todas as empresas envolvidas, dificultando processos de auditoria.

Essa dependência da tecnologia já vinha sendo observada com a adoção das redes corporativas. No caso do EDI, estamos falando de uma interdependência entre empresas, o que muda bastante as estratégias em relação aos parceiros de negócios, clientes e fornecedores. Entra em cena uma cobrança mútua em relação a questões de qualidade e de segurança.

O Comércio Eletrônico também provoca uma mudança na estrutura de distribuição das empresas. As tradicionais redes de vendas, baseadas em lugares físicos e pessoal especializado, estão sendo substituídas por redes muito mais dinâmicas, com a eliminação de alguns intermediários no processo.

Outro ponto importante é que as empresas estão percebendo o Comércio Eletrônico como uma ferramenta básica para a redução de custos, redução do ciclo de desenvolvimento de produtos e melhora geral do fluxo de informação, entre outras coisas. Além disso, o uso desta tecnologia permite remover as barreiras de distância bem como viabiliza a virtualização das empresas (ALMEIDA, 2000).

Em relação às mudanças internas, as grandes empresas também estão adotando o Comércio Eletrônico para as suas redes internas (as chamadas *Intranets*), seus processos e aplicações. Albertin (1999) chama este processo de "Comércio Eletrônico interno (ou privado)", que utiliza as tecnologias de rede e o formato da Internet, de maneira que diferentes departamentos e setores das empresas automatizem seus processos de negócio.

Atualmente, com os custos bastante elevados das tecnologias de redes e Internet, necessárias para a manutenção do Comércio Eletrônico, e para a contratação do desenvolvimento dos sistemas e *sites*, uma nova tendência surgiu de forma a viabilizar a infra-estrutura tecnológica para as empresas que queiram implantar soluções de *e-commerce*. São os *Internet Data Centers*, ou IDCs.

De acordo com o *International Data Corporation* (BUSTAMANTE, 2001), *Internet Data Center*, ou IDC, é a denominação utilizada para se tratar os *Hosting Centers* ou *Hosting Providers*, que são enormes centros de dados preparados tecnicamente para hospedar uma grande quantidade de equipamentos voltados para a *Web*, tais como servidores, *storage* e equipamentos de conexão que enfocam aplicações de Internet.

Nos Estados Unidos, atualmente, existem cerca de 170 grandes IDCs em funcionamento, representando em 2002 um faturamento de US$ 2,49 bilhões (CERIONI, 2003). No Brasil, as primeiras empresas desse tipo começaram a surgir no segundo semestre de 2000, sendo que atualmente existem aproximadamente 21 grandes IDCs em funcionamento no país. Segundo o *International Data Corporation*, no ano de 2002 foi obtido um faturamento de US$ 83 milhões para o setor no Brasil (SOARES, 2002).

Segundo Oliveira (2000), os *Data Centers* são uma boa alternativa para as empresas que pretendem atuar nos negócios virtuais, mas não possuem as condições para realizar os grandes investimentos em infra-estrutura e pessoal de tecnologia. Uma outra vantagem diz respeito à segurança, já que os IDCs atuais ficam responsáveis por todas as tecnologias e recursos humanos necessários para questões de Segurança da

Informação e serviços de Comércio Eletrônico. A seguir, veremos quais são essas necessidades.

2.2.3 Segurança

Tomar a decisão de implantar uma solução de Comércio Eletrônico em uma companhia, hoje, parece por demais tentador. Implementar um serviço deste tipo com qualidade e segurança é bem mais complexo. Assim como em relação às redes corporativas, implantar um serviço de Comércio Eletrônico implica em um investimento sério em infra-estrutura de *hardware*, *software* e pessoal capacitado. E acima de tudo, requer uma preocupação obrigatória com a segurança. Por exemplo, em relação ao B2C, um dos problemas das compras pela Internet é a dificuldade em convencer as pessoas de que isto é seguro. Mais difícil ainda é fazer de fato com que tudo se processe de forma segura, e planejar ações para o caso de surpresas desagradáveis.

Nesse sentido, o Comércio Eletrônico, em todos os seus modelos de negócios (B2C, B2B, B2G, etc.), está intrinsecamente relacionado com a segurança. Sem um ambiente seguro e confiável, torna-se impossível realizar trocas comerciais, seja no mundo real como no virtual.

Almeida (2000) destaca aspectos de segurança relacionados ao Comércio Eletrônico, tais como **disponibilidade**, **confidencialidade** e **integridade** dos sistemas de informação e dos dados que são armazenados e transmitidos, conceitos que serão tratados no capítulo 5.

No caso do EDI, por exemplo, existe uma série de questões legais referentes a contratos e responsabilidades sobre transações, já que não há (ainda) referências legais ao uso de documentos eletrônicos, gerando ambigüidades na lei e reticência por parte das empresas. Estas também costumam ficar temerosas com relação à proteção e sigilo dos dados trafegados.

O mercado de B2B certamente é o que mais interessa às empresas de Segurança da Informação, já que em geral as duas pontas envolvidas nas transações (que são companhias) estão dispostas a pagar para utilizarem um ambiente de negócios mais seguro. O volume de dinheiro neste modelo também é bem maior do que no B2C.

Tigre (2003) realizou uma pesquisa sobre a utilização do Comércio Eletrônico, envolvendo 68 empresas da indústria manufatureira, 68 firmas de distribuição e 64 bancos e companhias de seguros. A tabela a seguir exibe diferentes tipos de uso da Internet e o percentual das empresas pesquisadas que os utilizam (TIGRE, 2003):

Forma de uso da Internet	Percentual de empresas da amostra
Realizar vendas on-line	28,2
Assistência técnica e suporte pós-venda	23,1
Realizar compras on-line	54,9
Trocar dados operacionais com fornecedores	51,9
Trocar dados operacionais com clientes	49,2
Integração de processos de negócios com fornecedores e outros parceiros de negócios	48,8

Tabela 1 – Números do Comércio Eletrônico no Brasil

Fonte: Adaptado de Tigre (2003). Formas de Uso da Internet.

Pelos dados na tabela acima, podemos identificar as formas de uso da Internet do tipo B2C, que são a realização de vendas *on-line*, a assistência técnica e o suporte pós-venda, através das quais as empresas interagem com os seus consumidores finais, e as formas relativas ao B2B, que são as compras *on-line*, a troca de dados operacionais com fornecedores e clientes e a integração de processos de negócios com parceiros e fornecedores. Fica evidente a maior utilização do modelo B2B pela maioria das empresas, representando assim um nicho mais atrativo para a área de segurança.

Normalmente, o aspecto crítico em transações B2B está relacionado aos mecanismos de segurança necessários para garantir o controle de acesso aos dados da empresa e a integridade dos mesmos. Em geral, são implementadas VPNs, *firewalls* e certificação digital, como exemplo de algumas das tecnologias utilizadas para restringir o controle de acesso e garantir a confidencialidade das informações e a autenticidade dos usuários, e que serão apresentadas no capítulo 5.

Já no caso do B2C, o Comércio Eletrônico parece ser um mercado potencialmente lucrativo e promissor, mas ainda pouco explorado. A segurança é um dos principais obstáculos para que empresas e seus clientes sintam-se confortáveis no ambiente de compra e venda, segundo Albertin (1999). Um problema clássico neste tipo de transação é fazer com que as pessoas envolvidas tenham a garantia de que os vendedores ou compradores são de fato quem eles dizem ser, e que as informações trocadas na transação não serão vistas por outras pessoas ou até mesmo adulteradas. Além disso, em relação ao comerciante, é preciso que a sua loja, ou seja, o seu *site*, esteja sempre disponível, "no ar", para que não sofra com a perda nas vendas. Finalmente, é preciso garantir que o pagamento realizado seja real, ou que os participantes irão honrar os compromissos assumidos "virtualmente". Sem dúvida, o que ainda representa uma grande lacuna é a utilização em massa de diversas formas de pagamentos, que ocorrem através da rede.

Transações eletrônicas em geral representam um alto risco para os governos e seus bancos centrais, pois abrem enormes brechas para fraudes, roubos, evasão de taxas, perda de controle da qualidade da moeda no mercado, dentre outros problemas. Muito ainda se precisa discutir e evoluir neste campo.

O tratamento dessas questões de segurança exige um aparato de *software* e *hardware*, além de uma melhora na estrutura de redes que existe atualmente, ainda fortemente baseada nos padrões e tecnologias desenvolvidos na época da ARPANET. Em meio a este cenário, surge então um mercado de segurança potencialmente lucrativo, voltado para o Comércio Eletrônico.

2.3 Segurança da Informação no governo

Os governos representam clientes extremamente importantes para as empresas de Tecnologia da Informação em todo o mundo. Além de contarem com recursos e potencial para investirem em tecnologia de ponta, o Estado possui o dever de alavancar as indústrias de seus países, investindo na inovação tecnológica.

Veremos neste item como se dá essa relação da Tecnologia da Informação com os governos, que possuem suas redes de computadores institucionais e seu Comércio Eletrônico, mais conhecido como Governo Eletrônico.

2.3.1 Tecnologia da Informação e o Estado

Assim como na economia e nos mercados, os impactos do avanço tecnológico no Estado também têm sido bastante significativos. A informação pública, gratuita, abundante e acessível precisa ser encarada como um dos bens mais importantes que o Estado deve oferecer aos seus cidadãos. Ao mesmo tempo, é preciso evitar a tendência, historicamente predominante em nosso país, de favorecer as classes dominantes e instruídas em relação às questões como educação e cidadania, gerando uma exclusão social cada vez maior.

O uso da Internet e o atual contexto de globalização representam uma ameaça para os Estados desarticulados, mas também um desafio e uma oportunidade para os Estados eficientes e democráticos (PINTO e SANTANA, 2000).

Os países que não se preocuparam suficientemente com a inclusão digital dos seus cidadãos nas décadas de 1980 e 1990 estão sofrendo as conseqüências neste início

de século, por não possuírem estrutura, recursos e capacitação local para o ingresso na sociedade da informação.

Atualmente se reconhece, a nível mundial, a necessidade de se investir em infra-estrutura de telecomunicações. Governos do mundo inteiro estão traçando políticas e diretrizes com este objetivo, de maneira a posicionar suas economias e empresas no mercado global (ALMEIDA, 2000).

Ainda de acordo com Almeida (2000), o setor público é o principal comprador de bens e serviços, independente do país, por possuir um volume de compras superior a qualquer outro cliente. Entretanto a autora afirma que os processos de compra são em geral lentos e presos às restrições burocráticas.

Na pesquisa realizada pela Sociedade SOFTEX (2002), o governo federal também aparece como um mercado importante na área de *software*, porém instável no atual momento. Segundo a pesquisa, os gastos do governo em todos os segmentos da TI, projetados para 2003, foram menores do que os de 2002 (R$ 1,89 bilhões, contra R$ 3,124 bilhões do setor financeiro em 2001, por exemplo). Além disso, uma grande parte dos gastos com *software* é feita em benefício do próprio governo, já que este contrata a sua própria empresa, o SERPRO, para o desenvolvimento de sistemas, o que poderia estar sendo contratado com *software houses* nacionais. Quase R$ 600 milhões do orçamento da área para 2003 representavam contratos com o SERPRO (SOCIEDADE SOFTEX, 2002).

O governo pode e deve interferir mais na adoção de tecnologias, tanto com políticas de demanda, que têm por objetivo estimular a difusão de novas tecnologias no setor produtivo, na Administração Pública e na sociedade em geral, como com políticas de oferta, que visam promover a indústria local de equipamentos, *software* e serviços de telecomunicações, o que resulta no desenvolvimento da infra-estrutura local.

Em relação ao Comércio Eletrônico, os governos possuem um papel fundamental relativo a legislações, políticas nacionais, capacitação profissional e incentivo à indústria local. Porém, Almeida (2000) observa que, de uma forma geral, o Estado brasileiro ainda se porta como um "espectador" das forças de mercado nesta área.

2.3.2 Governo Eletrônico

A tecnologia de Comércio Eletrônico também pode ser utilizada no relacionamento da Administração Pública com os cidadãos, com outras empresas e

internamente entre os órgãos do próprio governo. É exatamente disto que trata o Governo Eletrônico.

O e-governo, como vem sendo chamado, faz parte de um processo de reestruturação da sociedade moderna, de um modelo industrial para um modelo informacional, que conforma uma nova arquitetura tecnológica, econômica, política, organizacional e de gestão coletiva.

De acordo com Fernandes (2001), o Governo Eletrônico envolve três tipos de transação:

- G2G: transações dentro do governo ou entre governos;
- G2B: transações entre governos e fornecedores;
- G2C: transações entre governos e cidadãos.

Poderíamos ver estas siglas acima como modelos de negócio ou *cases* particulares do Comércio Eletrônico, como já foi observado no item anterior, obviamente possuindo várias características próprias.

O Brasil possui uma posição privilegiada em relação ao potencial para Comércio Eletrônico e Governo Eletrônico, como bem coloca Almeida (2000), graças a uma grande quantidade de "internautas", ao perfil do "internauta" brasileiro, com grande penetração nas classes alta e média, à rapidez do crescimento do número de computadores no país, e ao fato de que muitos brasileiros já estão acostumados a sistemas como a declaração do imposto de renda por meio eletrônico.

O governo tem a responsabilidade de legislar sobre o Comércio Eletrônico de forma geral e promover o seu uso, de forma a manter-se competitivo no Comércio Internacional. Pinto e Santana (2000) colocam que o Poder Executivo Federal vem atuando nas seguintes principais linhas de ação para o Governo Eletrônico:

- Promover a universalização do acesso aos serviços;
- Estimular o acesso à Internet;
- Implantar uma infra-estrutura de TI avançada.

Já existem exemplos de sucesso do projeto de Governo Eletrônico a ser implantado no Brasil. Quase todas as repartições públicas federais possuem a sua página na *Web*, oferecendo algum tipo de serviço ao cidadão. Exemplos destes serviços são o envio da declaração do imposto de renda (www.receita.fazenda.gov.br), a utilização de urnas eletrônicas nas eleições, a obtenção de certidões negativas, a abertura e acompanhamento de processos previdenciários, a consulta à lista de medicamentos

genéricos e de medicamentos suspensos, dentre outros. A Comprasnet (www.comprasnet.gov.br) presta serviços e divulga informações sobre as licitações do governo federal.

O projeto Rede Governo tem como objetivo ser o portal de entrada para todas as páginas do governo federal na Internet, e teve a sua implantação em 1995. Através deste portal (www.redegoverno.gov.br), pode-se ter acesso a 641 páginas de serviços e 3.683 *sites* de informações, distribuídos por 31 grandes grupos temáticos. Além disso, o portal oferece uma ferramenta de pesquisa em assuntos variados da administração pública.

O diagnóstico inicial para a situação tecnológica do Governo Federal é de um conjunto de diversas redes isoladas, sendo que várias já prestam serviços aos cidadãos. As maiores necessidades ainda são a integração de todos estes sistemas e uma preocupação maior com as questões de segurança, principalmente quando o acesso a tais sistemas passa a ser público. É o que será visto a seguir.

2.3.3 Segurança

Na área de segurança, o papel do Estado é mais do que fundamental. Faz-se necessário o estabelecimento de políticas que não apenas fomentem o uso das Tecnologias da Informação, mas que também regulem o seu uso de uma maneira geral.

As necessidades aparecem principalmente no governo eletrônico, onde são fundamentais questões como: garantia de privacidade; segurança das transações e acessos; legalização das transações *on-line* através de assinatura digital; proteção legal para os direitos autorais dos dados, legislação trabalhista e criação de programas para capacitar novos profissionais de tecnologia; leis de comércio para o mercado *on-line*; defesa do consumidor; cobrança de taxas sobre o comércio na Internet; sistemas de pagamento e financiamento eletrônicos; dentre outras.

Em se tratando de cidadania, é desnecessário dizer que o sigilo e a confiabilidade são de extrema importância em operações que envolvem ganhos, propriedade e identificação (por exemplo, RG e CPF). A Segurança da Informação precisa ser garantida pelo Governo Eletrônico, de forma a prover, assim como no Comércio Eletrônico, a confiança para os usuários e a verdadeira democracia.

A transparência fiscal, uma característica exigida dos estados ditos democráticos, requer segurança dos processos, auditoria, responsabilização, controle de acesso, e uma série de outros critérios que fazem parte do ramo da Segurança da Informação, e que precisam ser definidos e aplicados com a máxima seriedade.

Yourdon (2002) comenta que, além da integração e coordenação dos dados de suas próprias empresas, promovidas pelo governo, existe um movimento atual, nos Estados Unidos, para encorajar as companhias do setor privado a compartilharem os seus dados relativos à segurança umas com as outras e com o próprio Estado. Medidas como estas podem ser mandatórias através de leis, como aconteceu com as companhias aéreas após os atentados de 11 de setembro.

No Brasil, já existem diversas ações em andamento no Governo Federal para a área de segurança, como o Programa Brasil Transparente e a Política de Gestão de Segurança da Informação, com o desenvolvimento de padrões para a certificação e autenticação eletrônicas. O programa ICP-Brasil (Infra-estrutura de Chaves Públicas), por exemplo, está tratando de criar uma infra-estrutura nacional para chaves públicas. A ICP-Brasil foi criada para garantir a autenticidade, integridade e validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (ICP-BRASIL, 17 out. 2003).

A idéia é que os documentos assinados com certificados ICP-Brasil sejam válidos juridicamente. Estes certificados poderão ser emitidos para pessoas físicas, jurídicas, e para equipamentos ou aplicações, e deverão ser aceitos nas aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores, os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS e da seguridade social.

O SPB[4] também representou uma explícita intervenção do governo no campo da segurança, ao definir uma série de requisitos de segurança a serem satisfeitos pelos bancos para que os mesmos pudessem participar das transações no sistema.

O sistema brasileiro de eleições eletrônicas, visto como uma referência no exterior, é um outro exemplo de aplicação do governo eletrônico, que envolve sérias e polêmicas questões de segurança. Atualmente, muito se discute a respeito dos critérios adotados para a garantia da segurança do processo eleitoral realizado com as urnas eletrônicas e com a apuração computacional.

---

[4] Sistema de Pagamentos Brasileiro: implantado em 22 de abril de 2002, foi um sucesso e um dos eventos mais marcantes na TI bancária brasileira. Desde a data da implantação do sistema, todas as transações acima de R$ 5.000,00 passaram a ser liquidadas no mesmo dia, e com muito mais segurança. O Banco Central monitora as operações bancárias *on-line* e administra a liquidez do sistema financeiro, diminuindo assim o risco sistêmico.

As empresas de Segurança da Informação possuem um grande nicho de mercado no Governo Eletrônico, e já estão há um bom tempo tirando proveito do mesmo. Isso pode ser visto nos projetos das eleições eletrônicas, da declaração de imposto de renda, e na segurança dos diversos *sites* existentes do governo. Quando for regulamentada a autenticação de documentos eletrônicos, diversas empresas irão disputar o desenvolvimento e implantação da tecnologia requerida para tal. Quando a certificação digital for uma realidade no Brasil, haverá muito serviço para a implementação das soluções em *software* e *hardware*. Certamente um mercado bastante lucrativo.

2.4 Segurança da Informação no mercado financeiro

Este item foi aqui incluído devido à grande importância que o segmento financeiro representa para a área de Segurança da Informação. De uma maneira geral, os bancos, privados ou estatais, e as demais empresas que lidam diretamente com o setor de finanças (financeiras, pregões, instituições de crédito, etc.) investem bastante em Tecnologia da Informação. É o que será visto a seguir.

2.4.1 A Tecnologia da Informação e o mercado financeiro

Se o governo é potencialmente o maior cliente de Tecnologia da Informação em todo mundo, as instituições financeiras, hoje em dia, representam os maiores investidores reais da área.

De acordo com Costabile e Azevedo (2003), não existem decisões estratégicas de negócios nos bancos atualmente que não considerem decisões de tecnologia. A TI faz parte integrante da formulação da estratégia das instituições. Lunardi *et al* (2001, p. 2), também apontam a área bancária como um dos setores que mais tem investido em TI, "tendo seus produtos e serviços fundamentalmente apoiados por ela".

O estudo feito pela Sociedade SOFTEX (2002) também mostra que algumas das principais oportunidades para as empresas nacionais de *software* estarão na área financeira:

> No setor privado, o setor financeiro é individualmente o maior e mais sofisticado mercado de *software*, tendo feito gastos em 2001 de mais de R$ 500 milhões em aquisição de *software* (de um total de R$ 1.347 milhões) (SOCIEDADE SOFTEX, 2002, p. 62).

Apesar de muito se investir em TI em todo o mundo, tem-se mostrado extremamente difícil apontar os efeitos destes investimentos nas organizações. É o

chamado ROI (*Return Of Investiments*). Lunardi *et al* (2001) afirmam que nas instituições financeiras, é muito mais fácil justificar tais investimentos. Os bancos atuam em um ambiente extremamente competitivo, onde a TI é um importante diferencial competitivo para a busca de clientes e aumento do volume de serviços prestados. Podemos dizer que os bancos atualmente estão dependentes da Tecnologia da Informação para criar produtos e serviços, estabelecer nichos de mercado e, ainda, lançar produtos antes de seus concorrentes. Lunardi *et al* (2001) ainda colocam que os executivos bancários têm justificado os elevados gastos em automação bancária muito mais em função da forte concorrência existente e, em menor proporção, pelos ganhos de economia de escala proporcionados pela TI.

No Brasil, bancos e Tecnologia da Informação sempre tiveram uma relação bidirecional de desenvolvimento. A informatização bancária brasileira teve início no final da década de 1970, quando se verificou uma demanda intensa para a automatização das agências. Naquela época, o banco brasileiro já era bem diferente dos modelos de outros países. A cobertura era nacional e não regional, como nos Estados Unidos, por exemplo, e a gama de serviços, muito maior (FEBRABAN, 2003).

No Brasil, o setor bancário é historicamente líder na adoção de Tecnologias da Informação, e os bancos brasileiros foram pioneiros na automação eletrônica, como afirma Tigre (2003, p. 7):

> A política de informática adotada no Brasil na década de 1980, apesar de suas dificuldades em estimular a competitividade da indústria, representou um forte estímulo para a capacitação tecnológica local, induzindo a entrada de alguns dos maiores bancos brasileiros (Itaú, Bradesco e Banco do Brasil) na produção de *hardware* e *software*.

Lunardi *et al* (2001), em sua pesquisa realizada em bancos do Brasil, Argentina, Uruguai e Chile (países do Cone Sul), observaram que a interação entre os altos executivos dos bancos e os executivos de TI é grande. Eles acreditam que este compartilhamento de visões entre os dois tipos de executivos é que tenha contribuído para a efetividade dos investimentos em TI realizados pela indústria bancária.

Com a Internet, os bancos começaram a ver no Comércio Eletrônico uma oportunidade valiosa de oferecer produtos e ganhar novos clientes. Tanembaum (1997), já citava a utilização da Internet por muitas pessoas, com o objetivo de pagar suas despesas, administrar suas contas bancárias e gerenciar seus investimentos. O *Internet*

Banking é atualmente oferecido por todos os bancos de varejo atuantes no Brasil, e tem se sofisticado a cada dia, quanto à oferta de produtos e de comodidades oferecidas.

A pesquisa de dados do setor financeiro, publicada no *site* da FEBRABAN (FEBRABAN, 20 nov. 2003), traz vários dados a respeito da importância do mercado financeiro para a Tecnologia da Informação. Segue um resumo destes dados:

- Em 2002, os bancos investiram R$ 3,5 bilhões em TI, correspondendo a um aumento de 13,2% em relação a 2001. Os *softwares* adquiridos de terceiros registraram a maior variação (37,3%), seguidos pelos desenvolvidos no próprio banco (23,5%) e pela aquisição de *hardware* (9,1%).
- Houve uma explosão na utilização do *Internet Banking*, com um salto de 177,9%, passando de 820,4 milhões de operações em 2001 para 2,28 bilhões de operações registradas em 2002.
- O número de clientes com acesso a Internet praticamente dobrou em dois anos (2000 a 2002), passando para 15 milhões de clientes.
- A implementação do SPB representou um impulso no mercado de TI bancária.

O dado mais significativo desta pesquisa diz respeito ao aumento extraordinário na utilização dos serviços de *Internet Banking* no Brasil. Independente das questões de segurança envolvidas no processo (que serão discutidas a seguir), as pessoas estão aderindo às inovações tecnológicas oferecidas pelos bancos.

De forma resumida, podemos afirmar que a Tecnologia da Informação age de forma a racionalizar os custos de operação a fim de tornar as instituições financeiras mais competitivas.

2.4.2 Segurança

Os bancos possuem uma preocupação natural com a segurança, desde os tempos em que a Tecnologia da Informação ainda não havia chegado às suas agências e cofres.

Quanto à importância da segurança para os bancos, Costabile e Azevedo (2003) argumentam que a mesma é fundamental, e que sempre será um problema, requerendo soluções globais. Segundo os autores, a segurança não evoluiu junto com a tecnologia e precisa ser encarada como prioridade. Dentre as questões citadas, estão a identificação do cliente, a criptografia e a autenticação de mensagens.

Segundo Yourdon (2002), existe um grande interesse das empresas financeiras em relação à segurança, e que especialistas nos Estados Unidos advogam a

implementação de uma estratégia que crie uma rede separada (*Bifurcated Internet*), de forma a se evitar os riscos associados à Internet pública.

A Internet é um canal bastante oportuno para transações em bancos de varejo, segundo Costabile e Azevedo (2003), e uma tendência tanto para as empresas quanto para os bancos. Isto trará um investimento contínuo em segurança, já que muitas questões relativas a essa área ainda estão indefinidas.

A FEBRABAN (2003) vê a computação móvel e os *smart cards* como as principais tecnologias emergentes. Isso concorda com a previsão de Yourdon (2002) sobre as duas áreas principais a serem afetadas por tecnologias de segurança, em curto prazo, em todo o mundo: um maior uso de *smart cards* para identificação nacional, e um maior uso de vigilância de atividades dos cidadãos e entre eles.

No capítulo a seguir, iremos analisar a Tecnologia da Informação no Brasil e de que forma as empresas nacionais estão posicionadas globalmente para atender a essas diversas necessidades relacionadas à tecnologia, em especial as necessidades de segurança.

3 TECNOLOGIA DA INFORMAÇÃO NO BRASIL

Após contextualizar o leitor nas necessidades de segurança que surgiram no mercado de Tecnologia da Informação, analisaremos neste capítulo a TI no Brasil, destacando os principais aspectos que nos interessam para este estudo. Focalizamos a indústria de *software*, devido ao seu importante potencial de inclusão do país na Sociedade da Informação mundial e sua estreita ligação com as tecnologias de Segurança da Informação.

3.1 O Brasil no tabuleiro mundial da tecnologia

> [...] é intuitivo que abrir a caixa-preta e manipular seu conteúdo gera muito mais conhecimento do que apenas operá-lo (FLEURY e FLEURY, 1997, p. 64).

O Brasil é dependente de tecnologias do primeiro mundo, isto é um fato. Já no final da década de 1970, e durante a de 1980, diversos autores escreveram sobre o tema da "dependência tecnológica", uma teoria que tenta explicar as relações de dominação entre países. Basicamente, a teoria da dependência destaca que as relações de dominação entre as nações estão intimamente ligadas com as relações econômicas e de investimentos.

Dentre os instrumentos de dominação, Tigre (1984) cita:

- O exercício de poder monopolístico por multinacionais nos países em desenvolvimento, impedindo que empresas locais entrem em seus próprios mercados domésticos;
- O papel da importação de tecnologia inibindo os esforços locais de P&D e o controle estrangeiro sobre acordos de licenciamento, o que pode impedir uma real transferência de tecnologia para o Terceiro Mundo.

Tigre (1984) também ressalta a falsa transferência tecnológica que costuma ser vendida pelas multinacionais aos países periféricos. O que na maioria das vezes ocorre é exatamente uma inibição do mercado local e dos avanços em P&D. Atividades nesta área ficam praticamente restritas aos países de origem das multinacionais ou às subsidiárias das mesmas, instaladas em países de primeiro mundo.

Por falta de incentivo do governo ou por terem uma visão equivocada e de curto prazo, muitas empresas brasileiras decidem adotar padrões e tecnologias do exterior. Segundo Tigre (1984), a simples importação de projetos e especificações de produtos cujo desenvolvimento poderia ser realizado internamente pode prejudicar o avanço da capacidade local de P&D. Lemos (1999) também aponta que é possível transferir ou comprar os conhecimentos codificados, mas não os tácitos e que sem estes, não se tem a chave para a decodificação dos conhecimentos adquiridos na compra de tecnologia.

Algumas empresas brasileiras optam por realizar "parcerias" com empresas estrangeiras, com o objetivo de efetuar uma transferência tecnológica. Porém essa transferência muitas vezes acaba não ocorrendo, sendo a estratégia uma faca de dois gumes. Vilarim (2002) comenta as parcerias com empresas estrangeiras no país:

> No Brasil, um fato ocorrido após o fim da Reserva de Mercado foi o estabelecimento de parcerias entre empresas brasileiras e estrangeiras. Por um lado, a empresa nacional pode se tornar um distribuidor de tecnologias da outra, um tipo de relação que muitas vezes pode tolher o potencial da empresa brasileira no desenvolvimento de novas tecnologias; por outro, pode permitir a abertura de "caixas-pretas" tecnológicas que contribuirão para o aprendizado organizacional da empresa (VILARIM, 2002, p. 42).

No contexto atual de acelerado processo de globalização e de facilidades trazidas pelas Tecnologias da Informação, tende-se a considerar desnecessário o investimento de governos nacionais na promoção de atividades de geração de conhecimento e inovação (LEMOS, 1999). Para os que compartilham desses argumentos, o processo de globalização também incluiria a geração, difusão e acesso a informações e conhecimentos por todo o mundo, uniformemente, e se tornaria inútil o investimento na abertura das "caixas pretas", citadas por Vilarim (2002), posto que os resultados das pesquisas mundiais estariam públicos e disponíveis internacionalmente.

Entretanto, a distribuição de conhecimento permanece desigual entre empresas, países e regiões, sendo ainda mais relevante que se realizem investimentos para aumentar nossa base de conhecimentos e informações e capacitar nossos recursos humanos. Os fatos não apontam para uma distribuição automática e igual do conhecimento, promovida pela globalização. O conhecimento certamente ficará restrito à esfera de empresas, setores, países e regiões que invistam pesadamente na capacitação de seus recursos humanos, de forma a criar um ambiente local capacitado para se adaptar às mudanças freqüentes que ocorrem em nível mundial (LEMOS, 1999).

Para se ter uma idéia da participação brasileira na industrialização global, podemos fazer uso das patentes industriais, como forma de medição. A inovação tecnológica e o registro de patentes industriais por várias empresas internacionais do mercado de Tecnologia da Informação são fatores de grande importância estratégica. As patentes tecnológicas fortalecem o poder de decisão tecnológico dos países onde as mesmas são registradas.

Maldonado (1999) define patentes tecnológicas da seguinte forma:

> [...] patente é um direito legal conferido por agência oficial, nacional ou regional (no caso do Brasil, o INPI) e confere ao patenteador um monopólio da invenção e de sua exploração comercial ou industrial, por um tempo limitado (variando de 15 a 20 anos) e sobre um determinado território (MALDONADO, 1999, p. 110).

Uma patente corresponde a um instrumento legal de apropriação do conhecimento e dos resultados de seu uso, e é uma boa fonte de dados para se avaliar as relações de dependência entre países. Por exemplo, um país pode ter um fluxo monetário bastante grande nas suas transações comerciais com outras nações, mas o número de patentes realmente registradas por empresas ou indivíduos daquele país é que de fato fornece uma interpretação mais precisa dos valores.

Uma análise sobre a propriedade de tecnologias no Brasil, feita por Maldonado (1999), mostra que as multinacionais desenvolvem tecnologias dentro do país, entretanto protegem as mesmas através de patentes. Numa visão global, a posição do Brasil no *ranking* de P&D não tem sido muito animadora nos últimos anos. A participação do país nos fluxos globais de tecnologia é bastante reduzida e vem decrescendo, segundo Maldonado (1999). A tabela a seguir mostra a distribuição de patentes industriais, depositadas no Brasil, por diferentes países:

País	Número de patentes*
Estados Unidos	155
Japão	85
Alemanha	55
Itália	51
Grã-Bretanha	47
França	40
Outros países da OCDE	79
Leste Europeu	4
Brasil	48
Outros	8
Total	572

Tabela 2 – Patentes de invenção depositadas no INPI, segundo a origem – 1990/96

Fonte: Adaptado de Maldonado (1999).

*** Que apresentaram mais de um titular**

Como se pode observar, das 572 patentes depositadas no INPI, de 1990 a 1996, apenas 8% (48 patentes) pertencem a pessoas residentes no Brasil, enquanto 74% são de propriedade de residentes dos países da OCDE (Estados Unidos e Japão, principalmente).

Outra forma de se avaliar a posição brasileira na economia global é através dos números das importações/exportações. Segundo Castells (1999), a participação do Brasil nas exportações mundiais em 1990 correspondia a apenas 0,97%, considerando produtos caracterizados pelo conteúdo científico. Por outro lado, entre 2000 e 2001, o país importou cerca de US$ 1 bilhão/ano em *software* (SOCIEDADE SOFTEX, 2002).

No item a seguir, veremos os principais fatores a serem levados em consideração para a reversão deste quadro.

3.2 Recursos, pesquisa e desenvolvimento

O passo inicial para a formação de pessoal qualificado na área de Tecnologia da Informação, no Brasil, foi tomado no início da década de 1960. Nesta época, o ITA (Instituto de Tecnologia Aeronáutica) serviu de padrão para a reforma universitária brasileira, introduzindo o ensino associado à pesquisa, o que até àquela época não existia. Foi o início da trilogia Educação-Pesquisa-Desenvolvimento (PACITTI, 2000).

Essa constatação é de grande importância, já que muitas empresas nacionais da área de TI surgiram de ex-alunos das universidades brasileiras. Como exemplo, "cerca de 90 empresas foram criadas por professores, funcionários e, principalmente, ex-alunos da Unicamp" (FÁVARO, 20 fev. 2004).

Lemos (1999) ressalta o papel das instituições de pesquisa e das universidades, que fornecem a base do desenvolvimento científico e tecnológico para a geração de conhecimentos e capacitação de pessoas. A expansão do ensino superior, tanto público quanto privado, foi a fonte para o surgimento de novas empresas de informática no Brasil e a difusão dos *softwares* junto a usuários.

A importância da pesquisa acadêmica para o desenvolvimento tecnológico do país é destacada a seguir por Marques (2003, p. 663):

> Na primeira metade da década de 1970 nas universidades brasileiras, professores, alunos de pós-graduação e pesquisadores projetaram diversos produtos de informática: *modems*, terminais de vídeo, terminais inteligentes, (precursores dos microcomputadores de hoje), processadores dedicados, compiladores, protocolos de comunicação. Nestes mesmos anos, alguns birôs

> estatais de processamento de dados – particularmente o SERPRO – investiram em laboratórios de desenvolvimento de produtos.

A Sociedade SOFTEX (2002) também cita a importância dos anos 1970 e 1980 para a constituição, no país, de uma base tecnológica e industrial, formada por universidades, pesquisadores, profissionais e empresas, e necessária para o desenvolvimento da Indústria Nacional de *Software* (que será analisada mais à frente).

No caso específico do Rio de Janeiro, objeto do estudo de casos deste trabalho, Vilarim (2002) destaca fatores sociais, que ele chama de "trajetória social", os quais deram à cidade uma importância de destaque para empresas de informática:

> Esta região, além de conter uma grande quantidade de empresas do setor, possui diversas instituições de ensino que oferecem cursos superiores nas áreas de Computação e Informática, fornecendo ao mercado de trabalho grande quantidade de profissionais (VILARIM, 2002, p. 39).

O autor ainda comenta que no Rio de Janeiro o sistema de ciência e tecnologia é um dos mais completos do país, com 13 universidades no estado, sendo a grande maioria públicas, e 54 centros de pesquisa e instituições tecnológicas.

Ainda assim, existe pouco espaço para as empresas voltadas para tecnologia no país. Segre e Rapkiewicz (2003) observam que, em geral, os postos de trabalho para os profissionais de informática se concentram nas empresas que não têm a computação como atividade fim. Em geral, nestas empresas, os profissionais não possuem o ambiente propício para inovar e pesquisar novas tecnologias, tendo como foco apenas a redução de custos na gestão de TI.

A falta de uma política séria de inserção profissional faz com que cada vez mais o país deixe de exportar tecnologia para exportar mão-de-obra qualificada. Segundo Tigre (1999), com o aumento da oferta por profissionais de TI no mundo desenvolvido, um movimento de imigração de pessoas altamente qualificadas para os Estados Unidos tem sido gerado. É fácil encontrar na Internet *sites* com ofertas de empregos de grande qualificação, para trabalhos no exterior. Muitos deles desejam inclusive candidatos com níveis de pós-graduação, algo ainda pouco valorizado nas empresas brasileiras (TIGRE, 1999).

Segre e Rapkiewicz (2003) ressaltam que, por um lado, o Brasil está exportando mão-de-obra qualificada na área de informática para as empresas de *software* norte-americanas e, por outro, evidencia-se um aumento de carência de profissionais em áreas como redes de computadores e Internet.

Para reverter este quadro, é bastante importante que a universidade se relacione mais com o ambiente empresarial. Uma das necessidades levantadas na pesquisa feita pela Sociedade SOFTEX (2002) é o fortalecimento de parte da P&D acadêmica integrada a demandas futuras de empresas e instituições. Isto sem dúvida é a chave para o desenvolvimento das empresas nacionais e da utilização de todo o potencial do ensino universitário brasileiro.

A seguir, veremos como o Estado brasileiro vem tentando ao longo dos anos intervir nestas questões, através de políticas voltadas para o desenvolvimento local de tecnologia.

3.3 Políticas governamentais para a área de Tecnologia da Informação

A estratégia mais comum utilizada pelos países que atualmente lideram os mercados de tecnologia no mundo é a política de incentivo e, em muitos casos, de proteção de mercados.

Fleury e Fleury (1997) colocam que proteger e estimular suas empresas a partir de políticas ativas deveria ser um interesse da nação brasileira, assim como ocorre nos países desenvolvidos. De fato, a única maneira de vencer a dependência tecnológica é através do sucesso das companhias nacionais[5], sobretudo as pequenas e médias, que em geral se vêm impossibilitadas de competir no mercado global, apenas com suas próprias forças.

Neste item, vamos analisar o histórico das políticas governamentais para *hardware* e *software* que ocorreram no Brasil desde os anos 1970.

3.3.1 A Reserva de Mercado para Informática

O caso mais significativo de política de informática ocorrido no Brasil foi o que ficou conhecido como Reserva de Mercado para Informática, nas décadas de 1970 e 1980. Esta política de informática seguia uma estratégia de reserva de mercado para *hardware*, protegendo a indústria nacional e buscando estimular as empresas a crescerem e inovarem, como foi colocado a seguir:

---

[5] Neste caso, referindo-se às empresas efetivamente nacionais, desconsiderando as subsidiárias de multinacionais localizadas no Brasil.

> O objetivo era o desenvolvimento tecnológico local através da introdução de barreiras-limite à incorporação de tecnologia importada, via empresas multinacionais presentes do mercado brasileiro (SOCIEDADE SOFTEX, 2002, p. 18).

Marques (2003) lembra que apesar do seu abandono em 1990 e da fama negativa que ronda a Reserva de Mercado para Informática que ocorreu no Brasil, um acompanhamento mais detalhado dos acontecimentos mostra que poucos anos antes do seu fim, "a reserva de mercado aparecia como um expediente de sucesso digno e surpreendente" (MARQUES, 2003, p. 659).

A expectativa era a de que nossas empresas desenvolvessem capacidades e inovassem. De fato, essa política trouxe resultados de sucesso para o país. Marques (2003) cita, por exemplo, que no começo da década de 1980 o Brasil foi um dos poucos países em que empresas sob controle local conseguiram suprir uma parte significativa do mercado interno de minicomputadores com marca e tecnologia própria.

O ponto interessante é que os engenheiros brasileiros estavam de fato realizando as fases completas de concepção e projeto dos sistemas de *hardware* e *software* básico dos minicomputadores, atividades de alto valor de conhecimento agregado. Nas palavras de Marques (2003, p. 659):

> A comparação entre as características técnicas dos sistemas de minicomputadores colocados no mercado pelas empresas brasileiras e as características dos sistemas então oferecidos no mercado internacional indicam o quanto as equipes brasileiras se aproximaram daquelas existentes no mundo desenvolvido no início dos anos 1980.

Os produtos da pesquisa realizada pelos engenheiros brasileiros na primeira metade da década de 1970 não eram invenções, mas sim engenharia reversa feita localmente, em cima daquilo que havia de mais atualizado no mercado internacional. A idéia era aprender a fazer tais produtos, de tal forma que os profissionais adquirissem a capacidade de projetá-los. Ou seja, abrir as tais caixas pretas, já citadas.

A preocupação da comunidade acadêmica na época (década de 1970) era a de que uma dependência cada vez maior dos computadores, sem se saber como construí-los, poderia ser bastante perigosa para o país no futuro, eventualmente obrigando os brasileiros a pagarem o preço que fosse fixado por um grupo privilegiado de países.

Um fato importante foi que essa comunidade de profissionais concluiu que o desenvolvimento de uma tecnologia de minicomputadores não seguiria adiante com sucesso sem o envolvimento de empresas nacionais privadas (MARQUES, 2003).

Entretanto, as empresas nacionais não queriam entrar neste mercado, pois entendiam que, "em regime chamado de 'livre concorrência', a competição estava perdida a *priori* para as empresas estrangeiras" (MARQUES, 2003, p. 667).

Foi a partir destes fatos que surgiu a idéia de uma Reserva de Mercado, como um instrumento para tornar o investimento em concepção e projeto local de minicomputadores no Brasil um negócio mais atraente. Dessa forma, em julho de 1976 o governo militar decretou a Política Nacional de Informática para minicomputadores, com o objetivo de consolidar um parque industrial com total domínio, controle da tecnologia e decisão no país.

Os competidores estrangeiros foram mantidos fora dos segmentos de mercado contemplados pela política com restrições às importações e ao investimento estrangeiro (SOCIEDADE SOFTEX, 2002).

Nesta época, ainda não existiam os microcomputadores, como lembra Marques (2003). A Reserva de Mercado fora até então fruto da troca de idéias entre a comunidade de professores, profissionais de tecnologia e militares. Na década de 1980, os militares assumiram o comando das decisões relativas ao futuro da Reserva de Mercado, excluindo a participação daquela comunidade inicial de cientistas. O microcomputador foi incluído no escopo da reserva, sem a realização de nenhuma mudança para atender as particularidades desta nova tecnologia. Com o aumento das pressões norte-americanas para a abertura do mercado brasileiro de tecnologia e da demanda interna para os microcomputadores, a Política Nacional de Informática começou a caminhar para o seu fim, que ocorreu oficialmente em 1990.

A Política Nacional de Informática privilegiou o *hardware*, tratando o mercado de *software* apenas como um subproduto das vendas de equipamentos (SOCIEDADE SOFTEX, 2002). Porém, já em 1991 o país contabilizava um mercado de *software* de US$ 1.1 bilhões, aproximadamente 1/3 do total de toda a Tecnologia da Informação produzida naquela data. Uma soma muito grande que não foi vislumbrada pela política nos anos 1970 e 1980, e que a partir dos anos 90 precisou entrar na pauta dos programas nacionais para TI. É o que veremos a seguir.

3.3.2 Políticas governamentais para a área de *software*

O fim da Reserva de Mercado para Informática reconfigurou o posicionamento das empresas no mercado, fazendo com que muitas delas deixassem de desenvolver *software* próprios e optassem por soluções vindas prontas do exterior (Vilarim, 2002).

Isso motivou a formulação de novas políticas governamentais, que incluíam incentivos para empresas multinacionais produzirem no Brasil e programas de fomento para as empresas locais se desenvolverem.

Alguns exemplos dessas políticas são apresentados a seguir (SOCIEDADE SOFTEX, 2002):

- Lei 8.248/91, que tinha como objetivo o estabelecimento de mecanismos alternativos para preservar a produção local e as atividades de P&D na Indústria de Informática, e que vigorou até o ano 2000.
- Projeto Desenvolvimento Estratégico da Informática – DESI, criado em 1992, e que tinha dentre os seus três programas o SOFTEX 2000 (Programa Nacional de *Software* para Exportação). O objetivo inicial do SOFTEX era estimular o surgimento de uma Indústria Brasileira de *Software* voltada para exportação e conquistar 1% do mercado internacional (ROSE, 1996).
- Sociedade SOFTEX, criada em 1996 como uma organização não-governamental com o objetivo de coordenar o programa SOFTEX 2000 e a sua rede de Agentes (22 cidades e 12 estados).

O SOFTEX 2000 posteriormente veio a se chamar Programa SOFTEX, e foi responsável pela disseminação da cultura do empreendedorismo nas companhias, a criação de uma linha de financiamento específica para as empresas de *software*, o PROSOFT, em parceria com o BNDES, além de promover a participação de 399 empresas em eventos internacionais. Atualmente, 37% das empresas de *softwares* brasileiras estão associadas ao Programa SOFTEX e, de 1990 a 2001, o programa contribuiu para o incremento da exportação de *software* brasileiro em quase US$ 100 milhões (SOCIEDADE SOFTEX, 2002).

Entretanto, o estudo realizado pela Sociedade SOFTEX (2002) mostra que o volume de recursos aportado no Programa SOFTEX ficou muito aquém do necessário para alavancar ganhos de escala comparáveis aos da Índia ou atingir um número de empresas compatível com uma estratégia focada em desenvolvimento de produtos como a da China. Devido a isso, mais recentemente o foco do programa deixou de ser a exportação, passando a ser a *excelência* no desenvolvimento de sistemas, com ênfase nas questões de qualidade. Ainda assim, a sigla do programa se manteve.

Instituições como SEBRAE, Assespro e Finep também atuam no fomento da indústria nacional de *software*, servindo como um intermediador de linhas de financiamento para as empresas do setor (FINANSOFT, 10 jan. 2004).

3.4 Desenvolvimento de *software*

3.4.1 O *software* no mundo

Nos primórdios da computação, o *hardware* era a peça chave da tecnologia, e representava o foco de investimentos em P&D, com o objetivo de melhorar o desempenho das operações de processamento. Com o avanço da tecnologia, o surgimento da eletrônica digital e um aumento significativo do poder computacional das máquinas, o *software* passou a ganhar importância.

Segundo dados da Sociedade SOFTEX (2002), o crescimento do mercado mundial de *software* e serviços relacionados deve passar de US$ 90 bilhões em 1997 para US$ 900 bilhões em 2008. Em 2001, esse mercado atingiu cerca de US$ 300 bilhões, sendo o Brasil responsável por 2,3% desse total. Mundialmente, os gastos de usuários finais em *software* devem crescer 3,6%, subindo de US$ 76,9 bilhões em 2002 para US$ 81,8 bilhões, em 2003. Produtos de *software* que ajudem a cortar custos, melhorar a segurança e integrar aplicativos existentes são os mais comprados. Entretanto, as grandes empresas estatais e privadas estão menos inclinadas a experimentar novas tecnologias, não testadas no mercado, ou apostar em tecnologias desenvolvidas por *start-ups*[6] (SOCIEDADE SOFTEX, 2002).

Portanto é inquestionável a importância que deve ser dada a este segmento da informática por uma nação que pretenda participar ativamente na economia mundial. Até empresas tradicionais de *hardware*, como a IBM, têm concentrado sua estratégia de crescimento em *software* e serviços, o que vem tornando a competição na indústria mundial de *software* cada vez mais acirrada (SOCIEDADE SOFTEX, 2002).

Menezes (2003) comenta que a indústria de *software* é considerada fundamental pela maioria dos governos, já que traz bilhões de dólares em receitas sem que nenhum recurso físico seja consumido. Além disso, *software* "gera imensos recursos na exportação, gera empregos de alto valor agregado, é uma indústria limpa e alavanca toda a cadeia de conhecimentos na sociedade" (MENEZES, 20 set. 2003).

As regiões que mais se destacaram na exportação de *software* são os grandes países desenvolvidos como os EUA e a Alemanha, que realizam atividades de elevado valor agregado e mais embasadas em P&D.

---

[6] Empresas formadas por poucos empreendedores, com capital próprio, e que surgiram a partir da identificação de uma oportunidade de mercado. Costumam ser gerenciadas de forma bastante amadora, contando com o entusiasmo dos sócios fundadores.

3.4.2 O *software* no Brasil

3.4.2.1 A indústria brasileira de *software*

A última pesquisa a respeito da Indústria de *Software* no Brasil, realizada pela Sociedade SOFTEX (2002), traz um quadro sobre a situação atual das empresas, dos profissionais e do nosso potencial para exportação. Apresentamos aqui seus principais pontos.

Foram coletados, através de entrevistas, dados de 57 empreendimentos selecionados dentre as empresas de *software* mais competitivas do país. Os critérios para a seleção foram (SOCIEDADE SOFTEX, 2002):

- Empresas com maior comercialização de *software*;
- Empresas reconhecidamente inovadoras no país;
- Empresas que receberam aporte de capital de risco;
- Empresas aprovadas nos critérios do PROSOFT.

Foi utilizada a classificação do BNDES para o tamanho das empresas, que se baseia no faturamento das mesmas (a qual utilizaremos também nos estudos de caso deste trabalho), e que apresentamos a seguir:

Tipo da empresa	Faturamento anual
Micro	até R$ 1,2 milhões
Pequena	entre R$ 1,2 e R$ 10,5 milhões
Média	entre R$ 10,5 e R$ 60 milhões
Grande	maior do que R$ 60 milhões

Tabela 3 – Classificação das empresas de acordo com o faturamento

Fonte: Elaboração própria a partir de dados da Sociedade SOFTEX (2002).

Na pesquisa, a atual indústria nacional de *software* é caracterizada por três destaques essenciais:

- Uma forte demanda doméstica que desestimula a exportação;
- Uma fragmentação do mercado nacional, com firmas de menor porte e avessas à cooperação;
- Uma inserção na economia mundial de Tecnologia da Informação mais desvinculada dos grandes centros (principalmente Estados Unidos).

Ainda assim, o Brasil é destacado como o sétimo mercado de *software* do mundo, tendo atingido vendas de US$ 7,7 bilhões em 2001. Entre 1991 e 2001, a participação do *software* como percentual do PIB nacional mais que triplicou, passando

de 0,27% para 0,71%. A sua participação no mercado de TI nacional como um todo aumentou em 2/3 (SOCIEDADE SOFTEX, 2002).

A maioria das empresas de *software* brasileiras possui várias linhas de negócio e desenvolve simultaneamente atividades de serviço e de produto, com uma maior ou menor preponderância de cada uma delas. Entretanto, a maior concentração está nos serviços. Sendo assim, com o objetivo de caracterizar as empresas, as mesmas foram divididas na pesquisa em diferentes modelos de negócios, que são resumidos na tabela a seguir (SOCIEDADE SOFTEX, 2002):

Modelo de Negócios	Descrição
Serviço de baixo valor	Envolve normalmente atividades tais como manutenção de *software* ou geração de código. Nesse caso, a gestão da empresa está voltada para a eficiência na gestão do processo. É a realidade atual das empresas indianas.
Serviço de alto valor	Envolve a incerteza relativa ao resultado ou a partilha de responsabilidade na definição do sistema (análise de requisitos). Um aspecto bastante importante neste modelo é a reputação. É um mercado dominado por empresas multinacionais de consultoria de sistemas, as quais possuem certificações do tipo ISO 9001:2000, CMM ou SPICE.
Produto/pacote	Este segmento é dominado por empresas multinacionais, principalmente pelo fato de exigir investimentos muito elevados antes que seja realizada a venda, tais como investimentos em pesquisa de mercado, inovação tecnológica e *marketing*. Os riscos são muito grandes, da mesma maneira que também são os retornos em caso de sucesso. Exemplos abrangem desde os produtos da Microsoft® (Windows® e Office®) até produtos específicos como ferramentas CAD.
Componente e *software* embarcado	Trata-se de produtos vendidos em conjunto com *hardware* ou *software* de outros fabricantes. A mitigação do risco é feita através da existência de um intermediário (no caso o tal fabricante) entre a empresa e o cliente final. Neste segmento, as empresas possuem uma tecnologia proprietária para consubstanciar o produto e uma relação estável com o intermediário, que confia o desenvolvimento do componente ao fornecedor. Exemplos são os sistemas de correção gramatical do Microsoft® Word®.
Produto customizável	Trata-se de soluções específicas para segmentos verticais, como, por exemplo, financeiro ou telecomunicações. O *software* envolve normalmente uma solução nuclear (*kernel*) que se mantém em todas as vendas, mas requer adaptação e desenvolvimento específico substancial para cada cliente. As adaptações podem ser feitas por terceiros. Mesmo tratando-se de produtos, o peso dos serviços nas receitas dessas empresas pode ser tão ou mais importante do que a venda das licenças. Um exemplo são as empresas de ERP.

Tabela 4 – Modelos de negócio da indústria brasileira de *software*

Fonte: Elaboração própria a partir de informações da Sociedade SOFTEX (2002).

As empresas brasileiras de segurança possuem seus modelos de negócio, em geral, voltados para **serviço de alto valor**, como é o caso das consultorias que desenvolvem soluções de segurança sob encomenda; e **produto/pacote**, como, por exemplo, os fabricantes de *firewalls* e sistemas antivírus. Mesmo assim, é possível encontrar empresas menores que prestam **serviço de baixo valor**, como revisão de código e busca por falhas de segurança. Algumas empresas brasileiras também se especializaram em nichos de mercado específico, como segurança para o mercado financeiro.

Destacamos a seguir as principais conclusões obtidas na pesquisa (SOCIEDADE SOFTEX, 2002), que estão mais relacionadas às empresas dos estudos de caso da presente dissertação, juntamente com resultados de trabalhos de outros autores. Algumas interpretações nossas também são realizadas.

Modelo de negócios:

As empresas de serviços de alto valor respondem por mais de 60% da comercialização total da amostra tomada na pesquisa (SOCIEDADE SOFTEX, 2002), seguidas por empresas em serviços de baixo valor. Apesar da maioria das empresas declarar sua atuação como focada em produtos, a análise da atuação verificou que são os serviços que predominam.

Empresas fundadas por empreendedores geralmente começaram com licença/distribuição de produto estrangeiro. Poucas, em período mais recente, surgiram a partir da identificação de oportunidade de mercado.

Atividade e nicho de atuação:

As pequenas e médias empresas geralmente buscam "produtizar" seu negócio, a partir da experiência adquirida com o desenvolvimento de *software* customizado em um nicho horizontal ou em um mercado vertical.

A pesquisa (SOCIEDADE SOFTEX, 2002) destaca que as empresas que entraram com um certo atraso em um novo mercado, como, por exemplo, o de segurança, vêm buscando a aquisição de competência através da compra de uma empresa menor (ou com competências e produtos em áreas complementares). Outras, buscando a expansão geográfica de seus mercados, têm multiplicado as parcerias de negócios ou adquirido empresas em novas regiões de expansão.

Localização:

A comercialização de *software* é feita por empresas concentradas na região Sudeste (87%), e os empregos gerados na área também estão, em sua maioria, nas regiões Sudeste e Centro-Oeste (54% e 23%). Em estudo realizado por Segre e Rapkiewicz (2003), também foi observada uma maior concentração de empregos formais para os profissionais de informática na região Sudeste.

Porte:

Em relação ao porte das organizações, 36% corresponde a empresas grandes, 35% a pequenas empresas, 22% a companhias de médio porte e, finalmente, 7% são micro empresas. Quase metade da amostra é fruto de empreendedores (*start-ups)*, o que é um dado surpreendente, já que na mesma pesquisa (SOCIEDADE SOFTEX, 2002), como citado anteriormente, também foi observado que as grandes empresas evitam comprar produtos e serviços destes novos empreendedores.

Segre e Rapkiewicz (2003) observaram de forma parecida que no Rio de Janeiro, assim como no restante do país, as firmas de informática tendem a ser caracterizadas como micro ou pequenas empresas. Além disso, as autoras destacam o número significativo (14,2%) de alunos formados no curso de informática da UFRJ que atuam em empresas próprias.

Pesquisa e Desenvolvimento:

A maior parte das firmas que derivaram de resultados de pesquisa acadêmica surgiu antes de 1980. A partir dos anos 1990, há um predomínio de empresas que se originaram de outras firmas, como decorrência dos processos de terceirização.

As empresas que trabalham em nichos específicos ou mercados verticais (como, por exemplo, o nicho de segurança e o mercado financeiro, respectivamente), representaram uma pequena quantidade da amostra. Mas, de acordo com a pesquisa (SOCIEDADE SOFTEX, 2002), são exatamente estas que se destacam na área de capacitação tecnológica e P&D.

A tecnologia empregada nas empresas foi, em sua maioria (62%) desenvolvida pela própria firma. Existe boa cooperação com a universidade, já que 40% das empresas têm acordos ou contratos para o desenvolvimento tecnológico. Apesar disso, a maioria (51%) relatou ir à universidade apenas para buscar recursos humanos.

As empresas de porte médio fizeram uso de incentivos fiscais para realizar investimentos em P&D, enquanto as de grande porte utilizaram programas governamentais. As empresas com foco em produto destacam-se dos outros segmentos em relação à magnitude dos recursos destinados à P&D e na geração da propriedade intelectual.

Metodologia e certificação:

A maioria das empresas atua no ciclo completo do desenvolvimento de *software*. Apenas uma pequena parcela das empresas possui certificação CMM nível três ou superior, sendo que destas, a maioria está associada a produtos. As empresas de serviço empregam metodologias próprias, mas sem certificação.

Exportações:

As empresas que fazem componentes e *software* embarcado participam com mais de 2/3 do valor total das exportações, seguidas pelas empresas de produtos customizáveis. Porém, apenas 13 das 45 empresas da amostra têm atividades de exportação ou de comercialização de seus produtos e serviços através de subsidiarias no exterior. A maior parte das exportações é feita através do uso de canais internos em multinacionais. Foi constatada também uma alta porcentagem de empresas de *software* com filiais no exterior (28%), em comparação com a média nacional. Essas empresas são, em geral, lideres em suas categorias.

Os *softwares* com maior valor agregado em serviços têm mais potencial para a exportação, como, por exemplo, os das áreas de telecomunicações, Governo Eletrônico, segurança de dados e redes, serviços financeiros ou varejo.

Aporte de capital:

O reinvestimento do capital próprio constitui a principal fonte de financiamento do crescimento das empresas. Outros financiamentos, tais como programas governamentais (PROSOFT, Finep e outros) e o capital de risco também têm adquirido uma expressão significativa nos últimos anos.

3.4.2.2 Destaques e barreiras

No estudo feito pela Sociedade SOFTEX (2002), foi identificada uma série de destaques positivos da indústria nacional de *software*. Os principais estão resumidos a seguir:

- Flexibilidade e criatividade das empresas, inclusive para a reorientação estratégica;
- Sofisticação dos mercados alvo das empresas, tais como setor bancário, telecomunicações, infra-estrutura energética e Governo Eletrônico. Produtos desenvolvidos para o SPB, liderado por empresas brasileiras, o sistema de

automação da receita federal e o sistema de compras governamentais são exemplos notáveis;

- Forte experiência na prestação de serviços para mercados verticais (segurança, por exemplo);
- Crescimento do uso da Internet.

Dentre os pontos fracos da indústria nacional de *software*, foram destacados os seguintes (SOCIEDADE SOFTEX, 2002):

- Existência de estrutura de regulamentação e política adversa ao desenvolvimento da indústria de *software* (Custo Brasil[7]), e ausência de incentivos à exportação;
- Limitada experiência das empresas em mercado aberto;
- Dificuldade de acesso ao capital de risco para investimentos;
- Mercado fragmentado, povoado por empresas de pequeno porte, pouco cooperativas;
- Grandes bancos privados ainda desenvolvem o *software in-house* e o governo federal compra relativamente pouco *software* no mercado;
- Governo parece não demonstrar um empenho forte no desenvolvimento da indústria de *software*;
- Altas taxas de pirataria de *software*, que impactam sobretudo as micro, pequenas e médias empresas;
- Ausência de um modelo e/ou imagem associados à capacidade do *software* brasileiro.

As principais barreiras ao desenvolvimento da indústria, segundo as empresas participantes da pesquisa (SOCIEDADE SOFTEX, 2002), dizem respeito à ação governamental, direta ou indiretamente. Já as grandes empresas citam a imagem do *software* brasileiro como a principal barreira. As micro e pequenas empresas se queixam do acesso ao capital, enquanto as médias destacam a falta de incentivos para exportação.

A tabela a seguir apresenta os resultados da pesquisa a esse respeito (SOCIEDADE SOFTEX, 2002):

---

[7] Termo utilizado para se referir ao custo de se ter uma empresa no Brasil, e, segundo Villela e Suzigan (1996), envolve fatores tais como carga tributária, legislação trabalhista, custo elevado de financiamento e altos custos relacionados aos trâmites burocráticos e regulatórios da atividade empresarial.

Tipo de barreira	Percentual das empresas
Preferência por tecnologia importada (no mercado interno) e desconhecimento do *Software* Brasileiro (no mercado externo).	38%
Acesso ao capital.	35%
Ausência de uma política industrial.	35%
Falta de mecanismos de incentivo à exportação (incentivos fiscais e facilidades).	33%
Compras governamentais.	29%
Baixa capacidade de *marketing*.	24%
Carga tributária incidente sobre os salários.	24%
Deficiência na interação entre universidade e empresa.	22%
Processos burocráticos (barreiras regulatórias, demora na liberação de financiamento e fraca atuação das embaixadas).	20%

Tabela 5 – Barreiras ao desenvolvimento da indústria de *software* brasileira

Fonte: Sociedade SOFTEX (2002).

3.4.3 Requisitos para novas políticas governamentais

A experiência adquirida com as políticas para a área de tecnologia no Brasil, analisadas nos itens anteriores, leva à identificação, por vários autores, de novos requisitos para os programas governamentais de fomento à indústria de TI.

Lemos (1999) observa que, atualmente, surge a necessidade de repensar políticas para o setor de TI, com foco no desenvolvimento individual de firmas, e as organizações e instituições envolvidas na formulação de tais políticas, para que as mesmas se adaptem às novas e dinâmicas necessidades de inovação.

Segundo Edwards (2001), a maioria dos países da América Latina, com o objetivo de melhorar as suas chances de crescimento, tem depositado as suas esperanças na expansão do papel da tecnologia, particularmente da Internet, e da Nova Economia. Entretanto, o autor argumenta que, de forma a tirar total vantagem das novas tecnologias, os países latino-americanos terão de fazer maiores investimentos em áreas complementares, incluindo P&D, educação e infra-estrutura. A razão para este fato é que a TI é uma "tecnologia de propósito geral", e seu impacto no crescimento do país depende não apenas de seu próprio nível de desenvolvimento, mas também no nível de desenvolvimento de outros fatores complementares.

Para o caso específico do *software*, uma política séria e efetiva deveria atentar para o seguinte (SOCIEDADE SOFTEX, 2002):

- Distinção entre serviços e produtos;
- O Estado deve usar o seu poder de compra para financiar a capacitação em processos e construir a reputação do *software* nacional;
- Desenvolvimento da capacidade empreendedora;

- Financiamento de custos de desenvolvimento e de *marketing*, barreiras quase que intransponíveis para micro e pequenas empresas em fase de crescimento.
- Fortalecimento da participação internacional das empresas brasileiras.
- Visão de crescimento sustentado e baseado em uma imagem brasileira forte no exterior.
- Investimento na formação de mão-de-obra.
- Em termos de competição internacional, focar em serviços de *software* com maior valor agregado, tais como segurança de dados e telecomunicações.
- O custo do emprego na indústria de *software* do país precisa ser reduzido para permitir que a competitividade salarial brasileira não fique exclusivamente atrelada a variações cambiais.
- A estrutura geral de impostos sobrecarrega empresas de todos os portes e ramos de atividades na indústria. Alguns estados e municípios brasileiros têm proporcionado incentivos fiscais, o que deve ser estimulado.

Após analisar o quadro brasileiro em que estão vivendo as empresas nacionais de tecnologia, no capítulo seguinte veremos as estratégias de gestão consideradas como as mais indicadas para estas empresas, inseridas no contexto da Nova Economia global.

4 ESTRATÉGIAS PARA AS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO

> Os subordinados sabem mais do que seus diretores em virtualmente todas as organizações. Durante períodos de intensa mudança, este paradoxo pode ser fatal (MICHAEL HAMMER, 2001 *apud* YOURDON, 2002, p.32).

Este capítulo apresenta os principais conceitos que estão envolvidos nas estratégias competitivas para as empresas da chamada Nova Economia, em especial as empresas de TI.

4.1 Conhecimento e estratégia

4.1.1 A Nova Economia

Ao se falar em estratégias empresariais para as companhias de TI, é preciso situar-se na indústria brasileira de tecnologia e novo contexto econômico mundial em que estas empresas estão inseridas. No capítulo anterior, tratamos de analisar a primeira parte, e, neste item, vamos nos concentrar no contexto desta Economia Baseada no Conhecimento.

4.1.1.1 Informação e conhecimento

Um dos traços mais marcantes da economia mundial nos dias de hoje é a importância da informação e do conhecimento. O que ficou conhecido como "Nova Economia", ou "Economia do Conhecimento", é uma nova realidade mundial em que o conhecimento passou a ter um valor muito maior do que os tradicionais bens de produção. Esse fato é conseqüência da maior disseminação das informações por todo o mundo, principalmente com o advento das Tecnologias da Informação e da globalização dos mercados.

Com essa imensa quantidade de informação disponível, é de grande importância saber gerir o conhecimento, para tirar proveito do mesmo. Vilarim (2002) diz que a gestão de conhecimento é uma estratégia vital das organizações para a sobrevivência nos dias de hoje, e que junto com a inovação e o empreendedorismo, o conhecimento forma o tripé da chamada "inteligência empresarial".

Estudos relativos a TI e desempenho econômico (EDWARDS, 2001), têm feito uma distinção entre a contribuição para o crescimento das empresas que "usam tecnologia" e das empresas que "produzem tecnologia". Uma importante conclusão destas análises – que, segundo o autor, possui implicações políticas para a América Latina – é que a contribuição das empresas que "produzem tecnologia" é significativamente superior em relação à das empresas que apenas "usam tecnologia". É importante destacarmos aqui que as empresas de Segurança da Informação que nos interessam neste estudo são aquelas que produzem tecnologia, e que podem resultar em uma inserção mundial do Brasil na Nova Economia.

Segundo Lemos (1999), e como já foi destacado no capítulo anterior, apenas poucas empresas ou países no mundo concentram as maiores taxas de investimento na geração de conhecimento – traduzido em atividades de pesquisa, desenvolvimento, educação e treinamento – e de inovações, representando a maior participação no ambiente competitivo mundial, enquanto outros permanecem marginais a esse processo. Como coloca a autora a seguir:

> Aponta-se para uma significativa concentração em nível mundial da taxa de introdução de inovações, com algumas regiões, setores e empresas tendendo a desempenhar o papel de principais indutores de inovações, enquanto outras parecem ser relegadas ao papel de adotantes (LEMOS, 1999, p. 137).

Na discussão sobre inovações, veremos quanto o conhecimento é importante neste processo de produção. Infelizmente, países que se concentrarem no consumo de Tecnologias da Informação, terão pouco a crescer. Neste sentido, não poderemos medir o avanço de países como o Brasil, na área tecnológica, somente pelo fato de seus habitantes estarem fazendo uso de tecnologias.

4.1.1.2 A nova competição

Com as novas tecnologias e a maior importância dada ao conhecimento, houve mudanças nas regras do jogo mundial, onde competem empresas nacionais, multinacionais ou transnacionais.

Uma das mudanças foi o aumento da competitividade, em nível internacional, como cita Castells (1999, p. 281-282):

> [...] o ponto principal no novo período histórico é que em um sistema econômico internacionalmente integrado, a expansão da demanda e da produção dependerá da competitividade de cada unidade econômica e de sua localização em um determinado cenário institucional.

Segundo Fleury e Fleury (1999), as três ondas de mudança que foram responsáveis pelas novas "regras do jogo" do mercado internacional são as seguintes:

- *Passagem de um regime de mercado vendedor para comprador*: nos anos 1970, a demanda era maior que a oferta, de forma que os produtos ditavam as regras no mercado. Com a crise do petróleo, essa situação começou a ser invertida, fazendo com que os clientes e consumidores passaram a ditar as regras;
- *Globalização dos mercados e da produção*: marcada pela desregulamentação dos mercados, avanço das Tecnologias de Informação e pela globalização produtiva, onde as empresas internacionais procuraram organizar-se segundo uma lógica de operações integrada globalmente;
- *Advento da economia baseada em conhecimento*: nesta economia, o que mais adiciona valor são as atividades inteligentes. As atividades rotineiras e manuais de produção passam a ser cada vez menos importantes, e podem ser exportadas para outros países, com mão-de-obra menos qualificada.

É dentro deste contexto que as empresas de TI cruzaram os anos 1980 e principalmente, os anos 1990, substituindo a busca por produtividade pela qualidade total. As técnicas de produção já estavam consolidadas, e os consumidores, mais exigentes.

As empresas encontram cada vez mais dificuldades para sobreviver em mercados fechados, onde possam dominar ou enfrentar apenas concorrentes locais. Para as empresas de tecnologia brasileiras, esse fator é ainda mais forte, já que as mesmas estavam acostumadas a um mercado protegido até a chegada dos anos 1990. A partir daí, houve a implantação de políticas de liberação de importações e um aumento do comércio exterior, fatos advindos em parte da pressão dos Estados Unidos para a abertura do mercado de informática brasileiro (SOCIEDADE SOFTEX, 2002).

Esse novo cenário de disputa mundial faz com que novas estratégias empresariais sejam pensadas e adotadas pelas empresas nacionais de Tecnologia da Informação, não apenas com um objetivo de aumento de produtividade ou lucratividade, mas também de sobrevivência. Vilarim (2002) coloca que é preciso entender o novo paradigma da flexibilidade, que, combinada com o acirramento da concorrência, com a desregulamentação e o fim do protecionismo governamental, com a mudança tecnológica em si, e ainda a valorização das necessidades dos clientes, fez com que as empresas de todo o mundo passassem a adotar novas estratégias.

Segundo Passos (1999), existe uma consciência cada vez maior a respeito das ameaças provocadas pela concorrência, de forma que algumas companhias chegam mesmo a contratar serviços de consultoria especializados em estratégias empresariais. Segundo o autor, estes serviços podem ajudar a empresa a aplicar de maneira mais racional os seus recursos, e a encontrar um foco de atuação no mercado.

Passos também cita a necessidade de se desmantelar as rígidas estruturas departamentais e promover, de um lado, a integração entre a pesquisa e desenvolvimento (P&D) de produto, *design*, *marketing* e vendas, e, de outro, a relação com os fornecedores, parceiros e consumidores da empresa.

As estratégias das empresas de TI precisam ser dinâmicas, pois se trata de um mercado extremamente dinâmico e repleto de surpresas. Muitas estratégias que estiveram em moda na década passada já estão sendo condenadas atualmente. Yourdon (2002) cita os argumentos de Michael Hammer (2001), o guru da "reengenharia de processos de negócios", a respeito dessa dinâmica e da necessidade de se planejar sempre:

> [...] antes dos ataques de 11 de setembro, Hammer nos lembra que cinco anos de planejamento estratégico criado pelos grandes negócios no período de 1990-1995 em geral não se anteciparam ou se "planejaram" para a crise financeira na Ásia, para a emergência da Internet/*Web*, para a introdução de sistemas integrados de ERP, para a emergência da integração *supply-chain*, para a criação do Euro, ou para as conseqüências da desregulamentação na indústria de energia, eventos que tiveram conseqüências enormes, e freqüentemente devastadoras, no final dos anos 1990 e no início da década corrente (YOURDON, 2002, p. 29).

As empresas da Nova Economia precisam ser capazes de não apenas formular estratégias, mas também fazer isso constantemente. As estratégias podem inclusive ser facilmente copiadas por concorrentes. Formular estratégias envolve planejamento e decisão constantes.

Toda a empresa precisa participar deste processo de elaboração de estratégias, e não apenas a diretoria. É o que Hammer (2001 *apud* YOURDON, 2002) alerta na citação introdutória deste capítulo. Para isso, é importante que as relações de trabalho sejam flexíveis, proporcionando liberdade, criatividade e dinamismo.

O desafio maior para as novas empresas está na identificação dos fatores críticos de sucesso no mercado e no negócio específico no qual a empresa se lançou, e na busca da melhor combinação de capacitações. Além disso, é necessária priorização e

balanceamento: os recursos são sempre limitados e não se pode ser ótimo em todas as áreas.

Passos (1999) coloca que é preciso se antecipar aos movimentos dos concorrentes e aos comportamentos e modificações financeiras, jurídicas e regulamentares relativas às questões empresariais e publicas, as quais possam afetar no curto, médio e longo prazo a economia da empresa. Isso parece essencial para as firmas nacionais nos dias de hoje, de instabilidade financeira mundial e das legislações governamentais do Brasil.

Como será visto mais à frente, as empresas de TI inseridas na Nova Economia precisam desenvolver permanentemente três fatores internos para a sua competitividade, o que Fleury e Fleury (1999) chamam de um círculo virtuoso constituído por:

- Definição de estratégia de negócio;
- Identificação das competências essenciais e das competências das várias áreas da empresa;
- Alinhamento das competências individuais com as competências essenciais e das áreas da empresa.

Além da preocupação com novas estratégias, é preciso que haja condições para a competitividade das empresas nacionais, como foi visto no capítulo 3. E isto não pode ser apenas responsabilidade dos empreendedores, e sim uma meta do Estado. Segundo Passos (1999), a competitividade das empresas que operam dentro do país e exportam constitui-se no núcleo essencial da projeção internacional das economias nacionais.

Como fatores externos à empresa para a competitividade, podemos citar (PASSOS, 1999):

- Macroeconômicos, tais como taxas de juros, oferta de crédito e taxa de câmbio.
- Políticos-institucionais, tais como tributação, poder de compra do Estado e esquemas de apoio ao risco tecnológico.
- Regulatórios, tais como políticas de proteção à propriedade intelectual, de proteção ao consumidor, de defesa da concorrência e legislação ambiental.
- Infra-estruturais, tais como disponibilidade, qualidade e custos dos transportes, das telecomunicações, da energia e de serviços tecnológicos.
- Sociais, tais como qualificação da mão-de-obra, políticas de educação e formação de recursos humanos, política trabalhista e de seguridade social.

- Internacionais, tais como tendências do comércio internacional, fluxos internacionais de capital, investimentos de risco e de tecnologia, acordos internacionais e políticas de comércio exterior.

A seguir, vamos analisar a importância de um processo de aprendizagem e cultura a ser definido dentro das empresas de TI, requisito importante para garantir a sua competitividade.

4.1.2 Competência e aprendizagem

4.1.2.1 Gestão por competências

A gestão de uma empresa através de suas competências passou a ser um tema bastante comum entre os executivos das empresas da Nova Economia, a partir da segunda metade da década de 1990. O que parecia ser uma grande novidade pode ser visto como um rótulo mais moderno para administrar uma realidade organizacional ainda fundada nos princípios do Taylorismo-Fordismo (FLEURY e FLEURY, 1999).

Neste trabalho, será utilizada a definição dada por Fleury e Fleury (1999) para competência, importante por ser comumente adotada pelos gerentes de recursos humanos:

> Conjunto de conhecimentos, habilidades, atitudes que afetam a maior parte do trabalho de uma pessoa, e que se relacionam com o desempenho no trabalho; a competência pode ser mensurada, quando comparada com padrões estabelecidos e desenvolvida por meio do treinamento (FLEURY e FLEURY, 1999, p. 19).

A idéia da gestão por competências é valorizar ao máximo as potencialidades dos funcionários de uma empresa, de acordo com critérios e métricas definidas. Para tal, os gerentes de recursos humanos definem um conjunto de competências, ditas essenciais, para a companhia, e apresentam este conjunto como um objetivo comum a ser perseguido por todos na empresa. Cada funcionário, então, é avaliado de acordo com essas competências.

Mas o que seriam essas competências essenciais? São aquelas intrinsecamente ligadas ao foco estratégico da empresa. Cada organização possui um número definido de competências essenciais a serem desenvolvidas por seus funcionários. É importante notar três pontos (FLEURY e FLEURY, 1999):

- É importante não confundir competência com qualificação profissional, conceito usualmente relativo ao cargo ou ao estoque de conhecimentos da pessoa. O

conceito de competência procura ir além do conceito de qualificação: refere-se à capacidade da pessoa assumir iniciativas, ir além das atividades prescritas, ser capaz de compreender e dominar novas situações no trabalho, ser responsável e ser reconhecida por isso;

- Competências devem ser contextualizadas. Em geral, cada funcionário da empresa possui um determinado grau (uma nota) para dada competência. O peso que essa nota possui vai depender da importância daquela competência dentro da função do indivíduo;
- As competências essenciais de uma empresa jamais devem ser terceirizadas. O próprio objetivo da terceirização é passar para outra organização tudo aquilo que fuja ao foco estratégico da companhia.

As competências essenciais estão relacionadas diretamente com a sobrevivência, em longo prazo, de uma empresa. A estratégia das empresas de Tecnologia da Informação, que são líderes em nível mundial, é focar em um pequeno número de competências essenciais, de acordo com a área de atuação. Para cada estratégia específica de uma empresa, existe uma competência forte requerida.

No item a seguir, veremos o processo de desenvolvimento da cultura e do aprendizado organizacional, importante na gestão das competências individuais e da organização como um todo.

4.1.2.2 Cultura e aprendizagem organizacional

Assim como as pessoas, toda iniciativa empresarial possui uma cultura que influi bastante na sua "vida" e no seu desenvolvimento. A cultura organizacional exerce importante influência no sucesso das empresas no mundo atual, da mesma forma que a bagagem cultural de um indivíduo é essencial para o seu desempenho na sociedade.

É através de sua cultura que uma empresa se torna apta a reagir de imediato perante as abruptas mudanças no mercado. Ou seja, através da cultura, a empresa se torna competitiva. Nesta cultura, é preciso levar em consideração as crenças e os valores das pessoas que fazem parte da empresa (FLEURY e FLEURY, 1997).

Segundo Passos (1999), o conhecimento e a compreensão de todo o processo produtivo são a chave da cultura de uma organização, e precisam estar ao alcance não apenas dos empresários, gerentes e quadros técnicos, mas também de todos os trabalhadores.

Para os indivíduos, a cultura é o resultado de um processo constante de aprendizagem. Com as organizações, a situação é a mesma. Empresas que estabelecem estratégias que levam em consideração a importância da cultura organizacional formam o que Fleury e Fleury (1997) chamam de *Learning Organizations*. Estas organizações precisam desenvolver uma "memória organizacional", onde as informações são estocadas e as experiências passadas, tanto as bem-sucedidas quanto as mal-sucedidas, devem ser de fácil recuperação e disponibilidade para as pessoas.

O objetivo do estabelecimento de uma memória organizacional é claro: uma empresa precisa ser capaz de existir independentemente deste ou daquele indivíduo. Os indivíduos são responsáveis por interpretações distintas dos problemas. A memória organizacional precisa de informações exatas e não ambíguas. Além disso, não se pode depender de pessoas que são as únicas a deterem o conhecimento de determinados processos, principalmente em empresas de TI, onde tais conhecimentos costumam fazer parte da vivência dos profissionais. Isso pode ser trágico no caso da saída de funcionários da companhia.

Para evitar esses tipos de problemas, as organizações que aprendem trabalham por projetos (Fleury e Fleury, 1997). Quando um projeto termina, a sua equipe assume um novo, ou então seus membros são alocados em diferentes equipes de projetos. Isto subverte a idéia de carreira e de desempenhos para dar todo o destaque ao trabalho coordenado da equipe, além de facilitar a mobilidade de mão-de-obra. O foco sai do indivíduo e passa para o processo.

Os recursos humanos, dessa forma, são vitais para a cultura de uma empresa. Mas precisam ser vistos dentro de um contexto de aprendizagem. Infelizmente, muitas empresas apenas desenvolvem programas de valorização destes recursos como propaganda interna, incompatível com a realidade. Como colocam Fleury e Fleury (1997, p. 26):

> "Nossos empregados constituem nosso maior patrimônio; nosso objetivo principal é valorizar nosso corpo de empregados". Tais declarações muitas vezes mascaram os reais valores da organização e servem quando muito para os discursos das tradicionais festas de natal.

Resumindo, a estratégia de gestão do conhecimento e da cultura organizacional envolve a conjugação de três processos:

- Aquisição e desenvolvimento de conhecimentos;
- Disseminação e construção de memórias;

- Processo coletivo de elaboração das competências necessárias à organização.

A seguir, veremos que a cultura de uma organização é essencial para criar nas empresas as condições necessárias onde possa ocorrer a inovação.

4.1.3 Inovação

4.1.3.1 Definições e conceitos

A estratégia de inovação é uma das mais importantes para garantir a competitividade no mercado de tecnologia. Atualmente, a inovação se mostra necessária para uma sobrevivência em longo prazo.

Vilarim (2002) adotou em seu estudo a definição proposta por Dosi, que considera inovação como "a busca, descoberta, experimentação, desenvolvimento, imitação e adoção de novos produtos, processos e novas técnicas organizacionais" (VILARIM, 2002, p. 16). Ou seja, não necessariamente a inovação precisa representar uma novidade tecnológica, mesmo em se tratando de empresas de tecnologia.

Lemos (1999) define, de forma geral, dois tipos de inovação:

- Radical: desenvolvimento e introdução de um novo produto, processo ou forma de organização da produção inteiramente nova. Pode representar uma ruptura estrutural com o padrão tecnológico anterior, originando novas industrias, setores e mercados. Pode gerar também redução de custos e aumento de qualidade em produtos já existentes. O desenvolvimento da microeletrônica foi um exemplo importante deste tipo de inovação.
- Incremental: refere-se à introdução de qualquer tipo de melhoria em um produto, processo ou organização da produção dentro de uma empresa, sem alteração na estrutura industrial. Geralmente essas inovações são imperceptíveis para o consumidor, mas podem gerar o crescimento da eficiência técnica, aumento da produtividade, redução de custos, aumento de qualidade e mudanças que possibilitem a ampliação das aplicações de um produto ou processo.

4.1.3.2 Fatores da inovação

Fatores Internos

A utilização da Tecnologia da Informação é um determinante na capacidade de inovação das empresas. Como foi visto no capítulo 2, os bancos em todo o mundo estão

fazendo uso da tecnologia para ganhar a clientela do concorrente, procurando sempre inovar com produtos de todo tipo, oferecendo mais informações ao cliente.

A aprendizagem constante e o investimento na gestão e disseminação do conhecimento são também importantes fatores. Lemos (1999) coloca que a inovação exige novos e cada vez maiores investimentos em pesquisa, desenvolvimento, educação e treinamento. Neste caso, a Tecnologia da Informação pura e simplesmente pode ser inútil caso não haja uma base capacitada na empresa para utilizá-las.

Segundo Vilarim (2002), os valores e as crenças da organização e a forma como a empresa é administrada, que formam a cultura organizacional (discutida anteriormente) e são essenciais para o desempenho dos recursos humanos, são muito importantes para a inovação. A cultura pode tanto facilitar como dificultar o processo de inovação, como coloca o autor:

> Valores, normas, histórias, heróis internos, casos de sucesso, linguagem, e muitos outros, são elementos de comunicação da cultura da empresa entre seus profissionais. Muitos destes elementos permeiam a organização desde a sua fundação, originados a partir das próprias percepções dos criadores da empresa, e podem ser fundamentados numa estratégia de inovação (VILARIM, 2002, p. 61).

Fatores externos

A inovação não precisa estar relacionada à criação de algo absolutamente novo, baseado em tecnologias avançadas, o que costuma ocorrer em grandes empresas que trabalham com tecnologia de ponta e possuem recursos financeiros suficientes para manter laboratórios e pesquisadores bem remunerados. Lemos (1999) reforça que conjuntos de empresas de menor porte e que atuam em setores mais tradicionais podem desenvolver um processo de aprendizado e de capacitação para as mudanças, principalmente se contarem com um suporte do Estado. A parceria com universidades pode ser bastante produtiva nestes casos.

Mas para competir com as grandes empresas, principalmente as multinacionais, as pequenas e médias empresas brasileiras precisam se articular, e não esperar apenas o auxílio por parte do governo. Isto se mostra mais importante ainda nos países em desenvolvimento. Como coloca Lemos (1999, p. 141):

> [...] é necessário se compreender que mesmo sendo a empresa o *locus* do processo de inovação, a mesma não inova sozinha e necessita de articulação com os demais agentes, tendo em vista este ser um processo interativo.

O local em que as empresas se desenvolvem e atuam também é um importante fator. Segundo Vilarim (2002), a inovação pode ser abordada como o resultado de uma cultura tecnológica e de um *know-how* historicamente constituído em um espaço. Foi o que aconteceu com as empresas de tecnologia estudadas pelo autor, que aproveitaram a cultura tecnológica existente na cidade do Rio de Janeiro. La Rovere (1999) também coloca que as redes de firmas (formadas através de parcerias estratégicas) podem servir como "catalisadoras de inovações", e que as características regionais definirão a dinâmica da atividade inovadora.

Depois de apresentar os principais assuntos e conceitos que permeiam as estratégias necessárias para a Nova Economia, vamos a seguir discutir o que são essas estratégias competitivas e quais os seus tipos.

4.1.4 Estratégias

A palavra estratégia costuma estar relacionada a jogos, competições ou ações militares. Talvez justamente por isso tenha ficado tão em moda nos tempos atuais, quando se fala de administração de empresas. A estratégia que interessa para este trabalho é aquela relacionada à competição no ambiente dos mercados globais, onde as fronteiras são cada vez mais tênues, as barreiras comerciais começam a se extinguir, e clientes e fornecedores podem estar em qualquer parte do planeta, como já foi discutido anteriormente.

Para Fleury e Fleury (1999), o desenvolvimento de estratégia é a "gestão do processo de aumentar conhecimento" (FLEURY e FLEURY, 1999, p. 41). Uma estratégia competitiva visa a estabelecer uma posição lucrativa e sustentável contra as forças que determinam a concorrência na indústria.

Vamos considerar dois níveis de decisões em relação à formulação de estratégias para uma empresa (FLEURY e FLEURY, 1999):

- Estratégia de negócios: em que tipo de negócio a empresa deve atuar e como vai competir?
- Estratégia funcional: como deve uma determinada função contribuir para a estratégia de negócios?

A função a que se referem os autores corresponde à competência principal a ser desenvolvida na organização, que pode estar relacionada às operações, produtos ou *marketing*. Sendo assim, os diferentes tipos de estratégia competitiva, definidos por Fleury e Fleury (1999), são os seguintes:

Excelência Operacional:

Uma empresa que adote a estratégia de excelência operacional procura oferecer ao mercado um produto que otimize a sua relação qualidade/preço. Ou seja, estamos falando de produtos padronizados do tipo *commodity*, os quais já estão sedimentados em todo o mundo, possuindo, inclusive, tabelas de preço globais.

As funções relacionadas às operações são as mais críticas neste tipo de estratégia. A excelência operacional começa desde o projeto do produto, otimizando as operações da empresa, com uma produção bastante enxuta, e os serviços de pós-venda (suporte e manutenção). Um exemplo de indústria que adota este tipo de estratégia são os fabricantes de "placa mãe" para microcomputadores.

Inovação em Produto:

O objetivo deste tipo de estratégia é o de criar novos conceitos de produtos para clientes ou segmentos de mercado definidos. A competência forte neste caso são os Produtos, com a implantação de laboratórios de Pesquisa e Desenvolvimento (P&D) dentro da empresa. Esta estratégia costuma ser a das indústrias de TI, principalmente aquelas que ditam os novos padrões de tecnologia, como os fabricantes de sistemas operacionais. Estas empresas vivem em uma busca contínua pela introdução de novos produtos no mercado, de forma que a função *marketing* também é de grande importância.

Tradicionalmente, a inovação seria caracterizada nas empresas através da existência de um departamento de P&D. Este é o típico caso da inovação em produto, onde uma equipe fica dedicada exclusivamente a criar novos produtos que possam ser bem sucedidos no mercado. Manter um departamento desse tipo é caro para a maioria das companhias, pois se trata de um investimento com retorno, na maioria das vezes, em longo prazo.

Orientada para Serviços:

Estratégia típica de empresas voltadas a atender os desejos de clientes específicos. A competência forte é o *marketing*, sendo que as competências de negócios, associadas às técnicas e às operacionais, também são importantes.

Não há necessidade de se buscar a otimização das condições de operação nem de desenvolver projetos radicalmente inovadores, como nos casos anteriores. Em contrapartida, o desenvolvimento de competências na área comercial e no

estabelecimento de parcerias é fundamental para a realização das estratégias de negócio. Como exemplo, podemos citar as *software houses* que desenvolvem sistemas e soluções específicas para seus clientes, e que precisam de parcerias para atuar com tecnologias ou atividades que fujam ao seu conhecimento.

A tabela a seguir apresenta o relacionamento entre as estratégias empresariais e as competências desenvolvidas:

Estratégia empresarial	Competências essenciais		
	Operações	Produto	*Marketing*
Excelência operacional	Manufatura classe mundial	Inovações incrementais	*Marketing* de produto para mercados de massa
Inovação em produto	*Scale up* de fabricação primária	Inovações radicais (*breakthrough*)	*Marketing* seletivo para mercados/clientes receptivos à inovação
Orientada para serviços	Manufatura ágil, flexível	Desenvolvimento de soluções e sistemas específicos	*Marketing* voltado a clientes específicos (customização)

Tabela 6 – Tipos de estratégia e formação de competências

Fonte: Fleury e Fleury (1999).

As caixas sombreadas na tabela correspondem à união entre o tipo de estratégia empresarial e a competência essencial requerida. As empresas consideradas de "manufatura classe mundial" são aquelas que atingiram níveis de desempenho ótimos nas suas operações, produzindo mais com o menor custo possível. As firmas responsáveis pelas "inovações radicais" estão em uma busca constante por novos conceitos e geralmente provocam rupturas com os padrões existentes. No último caso, o "*marketing* voltado a clientes específicos" representa as companhias que possuem relacionamentos bastante próximos e dedicados aos seus clientes, procurando atender às demandas destes da melhor maneira possível.

A classificação do tipo de estratégia empresarial nem sempre é tão evidente. Muitas vezes a organização parece combinar diferentes estratégias, ou transitar de uma para a outra. A escolha de uma estratégia está relacionada ao negócio, ou seja, distintos negócios de uma mesma corporação podem adotar diferentes estratégias.

No item a seguir, discutiremos os arranjos empresariais que podem representar uma forma dos empreendimentos brasileiros se organizarem para o desenvolvimento de estratégias competitivas, mesmo não possuindo o porte e os recursos necessários para tal.

4.2 Articulação na Nova Economia

4.2.1 Terceirização

Antes de discutir os arranjos empresariais, é importante apresentar a estratégia da terceirização, que tem tornado possível as parcerias entre diferentes empresas. A terceirização (*outsourcing*) de serviços foi uma estratégia dominante nas companhias durante os anos 1990. Na verdade, pode ser vista como um termo novo para classificar uma atividade bastante antiga, que é a subcontratação de trabalho. Ou seja, se um fornecedor é capaz de executar uma determinada atividade ou serviço com maior eficiência e a um custo menor, então este serviço é passível de terceirização (LIMA, 1996).

A terceirização tem sido uma das principais tendências de mercado dos últimos dez anos. O mercado de tecnologia, em particular o de informática, não poderia ficar de fora. As áreas mais terceirizadas no mercado americano costumam ser desenvolvimento de *software*, treinamento, consultoria, manutenção de *hardware* e *software*, comunicação de dados, gerenciamento de redes, integração e gerenciamento de sistemas.

Para o caso do desenvolvimento de *software* terceirizado, Lima (1996) destaca que este pode ser feito de duas formas: total, ou seja, integralmente executado pelo fornecedor, ou parcial, executado em parte pelo fornecedor e em parte pelo cliente. Neste segundo caso, geralmente a equipe de desenvolvimento da organização contratante é encarregada das fases de levantamento e análise, podendo algumas vezes completar também a fase de projeto, e o fornecedor fica com as duas outras fases do ciclo-de-vida de desenvolvimento de *software* (implementação e testes).

A principal vantagem da terceirização, sem dúvidas, está na redução de custos, relacionada principalmente aos recursos humanos. Como cita Lima (1996), devido à alta dinâmica da área de informática, contratar, treinar e manter profissionais é um desafio constante. Além disso, muitas organizações correm o risco de perder funcionários, após todos os investimentos realizados, para outras empresas, que simplesmente oferecem um maior salário. Com a terceirização, estes custos são transferidos para o fornecedor, que então passa a ser o responsável pelos mesmos.

Em relação às desvantagens, a falta de qualidade nos serviços prestados e os altos custos parecem ser as mais observadas. A primeira resulta de um não

conhecimento por parte da empresa terceira sobre o tipo de negócio do cliente, resultando em decisões muitas vezes irreversíveis, que podem deixar de gerar informações importantes ao desempenho da organização. As empresas contratantes esperam sempre uma qualidade superior no *software* terceirizado, o que é mais do que justo, porém quase sempre resulta em conflitos com seus contratados.

A segunda desvantagem costuma ocorrer principalmente com os contratos de longo prazo, na maioria das vezes em torno de dez anos. Neste caso, mudanças no negócio e evolução de tecnologias podem fazer com que as organizações promovam ajustes que não foram previstos anteriormente no contrato. O desenvolvimento de *software* é a atividade de informática mais propensa a mudanças nos requisitos estabelecidos inicialmente, e desta forma, à elevação de custos quando terceirizada.

Com a terceirização, as empresas de TI podem focar os seus esforços nas suas competências essenciais, racionalizando seus processos e eliminando toda e qualquer atividade não essencial. Isso é bastante importante para a realização de parcerias estratégicas, já que nenhuma empresa pode oferecer uma solução de TI de fato completa. Por exemplo, um fabricante de *hardware* pode estabelecer uma parceria com uma empresa de *software*, de forma a produzir os aplicativos embarcados nos seus produtos. No item a seguir, vamos analisar como podem se dar estes arranjos empresariais.

4.2.2 As redes de empresas

O aumento da concorrência fez com que as posições de domínio no tabuleiro mundial das organizações fossem alteradas. As margens de lucro gigantescas, conseguidas por muitas companhias, reduziram-se bastante, provocando uma onda mundial de corte de custos.

Também vimos nos itens anteriores que, para permanecer no mercado, foi preciso que as organizações buscassem novas estratégias, elevando assim os seus níveis de excelência. As empresas não podem mais ser vistas como ilhas auto-suficientes, verticais, atuando em todas as áreas e provendo todos os serviços de que necessitam. Para sobreviver no mercado atual, é preciso ser capaz de se relacionar com outras empresas, as quais possam complementar as atividades não essenciais. Este relacionamento, como cita Lima (1996), permite o compartilhamento de investimentos em tecnologia, infra-estrutura de produção e/ou de distribuição, ou ainda outras operações no âmbito dos negócios.

Marques e Segre (2003, p. 349) comentam que "a terceirização problematiza o tamanho da empresa". De fato, com a terceirização de serviços que fujam à competência essencial da firma, é possível se articular em redes e "aumentar" o tamanho das empresas, com o objetivo de tornar-se mais competitivo em um mercado de concorrência internacional. Aliar-se a empresas ou grupos empresariais locais pode ser, em última análise, a chance de sobrevivência de muitas firmas.

Lemos (1999) considera a formação de redes como o formato organizacional mais adequado para promover o aprendizado intensivo para a geração de conhecimento e inovações. Assim, considera elementos de influência no desenvolvimento e na capacidade de inovação:

- Os variados formatos organizacionais em redes para promoção da interação entre diferentes agentes, nos quais mencionam-se, entre outros, alianças estratégicas, arranjos locais de empresas, *clusters* e distritos industriais;
- O ambiente onde estes agentes se estabelecem e interagem, como já foi visto anteriormente.

Lemos (1999) ainda coloca que, através das redes de empresas, é possível trocar idéias, responder e se adaptar às constantes mudanças no mercado e aperfeiçoar a produção e comercialização dos produtos desenvolvidos dentro do país. Estas redes podem envolver várias empresas, instituições de ensino e pesquisa, programas de fomento, governos, investidores, associações de trabalhadores, dentre outros.

A articulação de empresas em redes pode ser feita através de parcerias estratégicas. É problemático competir individualmente e, entretanto, as empresas brasileiras não estão habituadas a esta cooperação. Por exemplo, na pesquisa realizada pela Sociedade SOFTEX (2002), foi observado que existe pouca cooperação entre as empresas brasileiras de *software* pesquisadas (apenas 1/5).

Neste processo de cooperação, Fleury e Fleury (1999) colocam que o suporte das organizações governamentais é de grande importância, principalmente para possibilitar a inovação nas pequenas e médias empresas. No item a seguir, discutiremos a importância destas PMEs para o desenvolvimento tecnológico do país.

4.2.3 As pequenas e médias empresas

Nos países desenvolvidos, as pequenas e médias empresas (PMEs) representam o cerne do empreendedorismo, o motor do capitalismo e da livre iniciativa. Sem apoio a

estas empresas, o sistema fica concentrado em grandes monopólios empresariais, e o mercado, pouco criativo para o consumidor.

Edwards (2001) comenta que um fator chave para a competitividade é o suporte ao empreendedorismo. Os países que facilitam o lançamento de novos empreendimentos e companhias possuem uma vantagem maior em atrair investimentos para TI, por exemplo, e em fazer um uso efetivo destas tecnologias. Diversas políticas de apoio às PMEs vêm sendo assim implementadas nos países desenvolvidos, devido ao reconhecimento de que estas firmas podem ser potencialmente difusoras de inovações e também estimular o crescimento regional.

No Brasil, as PMEs são responsáveis pelo maior número de empregos criados. Apesar disso, as políticas governamentais parecem não favorecer estes tipos de empreendimentos. Até meados dos anos 1970, as PMEs tinham um papel pequeno no debate sobre o desenvolvimento econômico devido ao predomínio do paradigma da produção em massa (LA ROVERE, 1999). Com a difusão do modelo de especialização flexível, estas empresas passaram a ter um papel mais relevante.

O potencial das PMEs em estimular o desenvolvimento de uma região tem sido uma das bases das políticas de inovação dirigidas a essas empresas. Além disso, a região é importante na determinação do potencial competitivo das PMEs (LA ROVERE, 1999). É o caso do Vale do Silício, no estado da Califórnia (EUA), que é uma região formada por grande número de pequenos e médios empreendimentos de TI (além dos gigantes já conhecidos), e que detém uma economia avassaladora.

Uma das estratégias mais importantes para a inovação na área de TI, como já foi citado anteriormente, é a pesquisa e o desenvolvimento. Entretanto, atualmente os gastos com P&D estão cada vez menores nas pequenas e médias empresas, devido à falta de recursos financeiros nestas companhias. Yourdon (2002) lembra que apenas grandes empresas, tais como IBM e HP, podem estar investindo grandes somas em P&D, bem em meio a uma recessão econômica, como a atual, de forma a conseguir uma posição privilegiada mais à frente.

As grandes empresas possuem uma série de vantagens para inovar, tais como: maior acesso a crédito; economias de escala em P&D; maior poder político; maiores chances de desenvolver e implementar as tecnologias que serão dominantes na indústria. As PMEs, ao contrário, possuem condições de crédito menos favoráveis que as grandes empresas e, portanto, são mais sensíveis aos ciclos econômicos.

As PMEs, segundo Passos (1999), contam com a flexibilidade e com um risco muito menor que as grandes corporações, mas isso não é suficiente. Sem um suporte local para o desenvolvimento dessas empresas, que envolve desde investimentos a fundo perdido, sistemas tributários mais adequados ao tamanho das empresas, e um estímulo à articulação em redes, parece ser difícil que essas companhias consigam inovar e, até mesmo, sobreviver em longo prazo.

La Rovere (1999) coloca que as políticas de inovação voltadas para pequenas e médias empresas precisam dar a elas condições para superar suas limitações. A autora divide as políticas para PMEs em dois tipos:

- Políticas de oferta: focadas nos recursos (materiais e humanos) das empresas. Inclui o fortalecimento da capacidade tecnológica das firmas, com o apoio a atividades de P&D, interação universidade/empresa, e política de patentes e de compras do governo.
- Políticas de demanda: visam estimular o uso de novas tecnologias, encorajando o uso destas. Envolvem treinamento de usuários, provisão de serviços de consultoria em administração e informações às firmas, constituição de centros de informação tecnológica e apoio à formação de redes de firmas.

4.3 Estratégias empresariais no Brasil

Vários centros universitários brasileiros possuem pesquisadores especializados em estudar estratégias, competitividade e inovação empresarial. Entretanto, muitas empresas de TI nacionais, principalmente as pequenas e médias, ainda vêem a palavra estratégia como um luxo muito caro para tempos de crise.

A visão de que a adoção de estratégias empresariais corretas é essencial para a sobrevivência no mercado é bastante recente nas organizações brasileiras, segundo Fleury e Fleury (1999). A primeira mudança observada nessas empresas, de forma a se reposicionar localmente em mercados globalizados, foi a adoção de estratégias de focalização e terceirização. Também é destacada a introdução de um padrão internacional de competição de preços e qualidade.

Na pesquisa feita pela Sociedade SOFTEX (2002), verificou-se, por exemplo, que as empresas de *software* de tamanho médio são as que possuem o maior índice de pessoal (CLT) alocado em atividades de gestão. Nas micro empresas, esse número ainda é pequeno, já que na maioria dos casos, são os próprios fundadores que realizam as

funções de gestão, independente de sua formação. Além disso, as empresas brasileiras de *software*, pequenas ou grandes, possuem dificuldades em definir um modelo de negócios claro e flexível e em realizar mudanças organizacionais necessárias à sua implementação.

4.3.1 Competitividade brasileira

Em termos de competitividade, existem muitas desvantagens para as empresas de tecnologia da América Latina. Edwards (2001) observa que a baixa qualidade da rede telefônica local, da estrutura das taxas telefônicas pagas e o abismo no progresso em relação a serviços de banda larga representam sérias barreiras à exploração das TIs na região.

Outro fator importante a ser analisado no Brasil é o incentivo ao empreendedorismo. Em uma pesquisa realizada por Djankov et al (2000 *apud* EDWARD, 2001), os resultados obtidos sugerem que, na maioria das nações latino-americanas, os custos de se criar uma nova companhia (*start-up costs*) são extremamente altos. A tabela a seguir apresenta estes resultados:

País	Custo (parcela do PIB *per capita*)	Número de passos necessários	Tempo (dias úteis)
Nova Zelândia	0,4%	3	17
Estados Unidos	1%	4	7
Canadá	1%	2	2
Chile	12%	12	78
Colômbia	12%	17	55
Peru	21%	14	171
Argentina	23%	12	71
México	57%	15	112
Brasil	67%	15	67
Bolívia	236%	20	82

Tabela 7 – Custos de criação de uma nova companhia: uma comparação internacional
Fonte: Adaptado de Edwards (2001).

Em relação aos três primeiros países da tabela, considerados desenvolvidos, as nações latino-americanas possuem uma grande distância. Para se abrir uma empresa no Brasil, leva-se 60 dias úteis a mais que o requerido para a mesma operação nos Estados Unidos. Em termos de burocracia, são necessários 15 passos para se obter todas as permissões exigidas na abertura de um novo empreendimento no Brasil, cinco vezes mais que na Nova Zelândia. As questões de custo são mais assustadoras, já que se gasta algo perto de 67% do PIB *per capita* brasileiro na abertura de uma nova firma.

Um outro ponto bastante polêmico, e que também está relacionado ao que ficou conhecido como Custo Brasil, diz respeito às relações de trabalho. Autores como

Edwards (2001) consideram a legislação trabalhista na América Latina em geral rígida e que a mesma não facilita a rápida recolocação de trabalhadores através das diversas companhias e setores. Na visão do autor, em muitos países, as práticas de negociação trabalhista são centralizadas, ainda da era industrial, e tendem a ignorar as peculiaridades de empresas específicas, que em meio à mudança tecnológica podem se deparar com circunstancias particulares.

Os maiores trunfos competitivos do empreendedorismo brasileiro, observados no estudo feito pela Sociedade SOFTEX (2002), devem-se à criatividade dos profissionais para desenvolver soluções que atendam sua diversidade de demandas e a capacidade das empresas em integrar produtos e serviços nas suas soluções.

Um outro componente importante das estratégias das empresas de tecnologia no Brasil é a internacionalização (FLEURY e FLEURY, 1999). Com as recentes fusões e aquisições, algumas empresas estão ganhando escala para se aventurar fora do país. Em muitos casos, as fusões e aquisições representam uma tentativa de sobrevivência no mercado. Essas aquisições são em muitos casos essenciais para a exportação e atuação no mercado exterior, já que programas do governo têm se mostrado fracos em assumir esta responsabilidade. Porém, as aquisições e fusões também podem interferir muito nas empresas agregadas, representando até mesmo o fechamento de algumas delas.

Segundo a pesquisa feita pela Sociedade SOFTEX (2002), o capital de risco público e os programas governamentais, como o PROSOFT, têm tido um papel importante na modernização da gestão e na orientação estratégica para o crescimento das empresas brasileiras de *Software*.

4.3.2 Inovação no Brasil

Devido às barreiras que se impõem à competitividade das empresas brasileiras, discutidas no item anterior, e à desvantagem econômica dessas empresas para com o resto do mundo, a inovação tecnológica, focada em P&D, acaba por não ter grande presença no país.

Em sua pesquisa, Vilarim (2002) observou que a competição em TI no ambiente específico do Rio de Janeiro é forte, devido ao grande número de empresas de informática e à atuação de empresas de outros estados. A maioria das companhias estudadas pelo autor não possui um processo de inovação sistemático inserido na sua estrutura e estratégia empresariais. Em contrapartida, foram observados diferentes níveis de inovação informal. Casos de inovação de produto, como *software,* e de

inovação em processos, como o recrutamento de recursos humanos. Também foram observadas inovações de mercado, já que algumas empresas, como as de Segurança da Informação, descobriram nichos específicos e conseguiram ser bem sucedidas nos mesmos.

Vilarim (2002) também observou que, na maioria das empresas cariocas de TI, o conhecimento está na cabeça das pessoas, sendo os recursos humanos uma parte essencial da inovação. No caso específico de empresas prestadoras de serviços, em especial aquelas de serviços baseados em conhecimento, o processo de inovação é intimamente relacionado aos seus recursos humanos.

No que diz respeito à relação das empresas com entidades de fomento, tais como RioSoft, a mesma foi considerada fraca na pesquisa. Nos casos de vinculo com a entidade, o mesmo se deu principalmente devido ao *marketing* proporcionado. Além disso, os empresários entrevistados demonstraram um descontentamento em relação aos rumos tomados pelo programa Softex 2000, cujo foco se desviou da exportação de *software*, como foi citado no capítulo 3.

A pesquisa também destacou a importância da existência de uma comunidade informata no Rio de Janeiro, de pessoas que estudaram juntas e acabaram por formar uma empresa, e do perfil das firmas de tecnologia no Rio de Janeiro, que se deve principalmente a esta comunidade de profissionais. Vilarim (2002) apontou para uma grande carência em relação à formação de redes de empresas e ao fomento às pequenas e médias empresas, o que precisa ser mais bem explorado no país.

Lemos (1999) também ressalta a importância de formatos organizacionais baseados na proximidade local, como os *clusters* e distritos industriais, estruturados em redes locais de cooperação. Este poderia ser o caso de localidades como a cidade do Rio de Janeiro, que reúne várias empresas de *software*, criando um ambiente de confiança maior entre os empresários para a realização de parcerias, devido à proximidade dos agentes.

4.3.3 Estratégias de articulação global

Nos itens anteriores, foi possível ver que existe grande dificuldade em inovar por parte das empresas nacionais, muito devido à pouca cooperação entre as mesmas e pelas dificuldades enfrentadas principalmente pelas PMEs. Por outro lado, a inserção do Brasil na indústria mundial de tecnologia vem se dando através de parcerias com empresas estrangeiras, ou até mesmo pela aquisição das empresas nacionais por grupos

estrangeiros. Como foi visto no capítulo 3, poucas empresas de *software* conseguem exportar seus produtos com esforço próprio ou com a ajuda de programas de fomento.

No item 4.1.1.2, vimos que a intensificação do processo de globalização produtiva e a abertura às importações fizeram com que as empresas nacionais precisassem se reposicionar. A principal estratégia utilizada nesse processo foi a articulação em cadeias de produção globais, formadas por empresas de todo o mundo. Fleury e Fleury (1999) propõem a seguinte classificação para as empresas nacionais, de acordo com o seu posicionamento global:

		Tipo A Parceria em redes globais	**Tipo B** Inserção em cadeias produtivas globais	**Tipo C** Atuação em mercados não globalizados
Decisões de Re (configuração)		Tem capacitações que a tornam reconhecida no plano internacional; tem condições de negociar em relativa igualdade.	A estratégia de negócios é definida a partir do papel desempenhado numa cadeia com hierarquia e estrutura de governança; pequenas possibilidades de atuação em nichos alternativos.	Manutenção de autonomia decisória; comportamento tradicional, conservador.
Decisões de Coordenação	**Estratégia de Manufatura**	Depende da rede para a produção local de produtos novos; independente na produção de produtos próprios.	Muito dependente da dinâmica da cadeia produtiva.	Estratégia não é relevante; iniciando Programas de Qualidade.
	Desenvolvimento de produtos	Dependente da rede para *breakthrough*; tem capacitação local para projetos plataforma e derivativos.	A capacitação para o desenvolvimento de sistemas/produtos vai definir a posição na hierarquia da rede.	Desenvolvido de acordo com critérios tradicionais, locais.
	Arquitetura Organizacional	Relativamente autônoma; desenvolve todas as funções; grande ênfase nas relações interempresariais.	Guarda características de complementaridade com as demais empresas da cadeia.	Estrutura tradicional; baixo nível de integração funcional.
	Sistemas de controle gerencial	Grande autonomia para a definição de sistemas e critérios.	Deve incorporar padrões definidos pelas empresas que comandam as cadeias.	Não é relevante (ainda).

Tabela 8 – Posicionamento das empresas brasileiras na economia globalizada

Fonte: Fleury e Fleury (1999).

Nesta tabela, podemos ver três tipos distintos de estratégias. No caso da estratégia do Tipo A, apesar da dependência para a criação de novos produtos que façam parte da cadeia de produção global, a empresa possui liberdade para o desenvolvimento dos seus próprios produtos, fora da rede. Estas firmas precisam possuir um sofisticado sistema de gestão e uma definição de processos, de forma a poder interagir no esquema decisório dos parceiros globais. Na área de desenvolvimento de *software*, por exemplo, é necessária, além dos requisitos de gestão estratégica, a

existência de certificações como o CMM, por exemplo, de forma a tornar a empresa um referencial internacional na área.

As empresas do Tipo B funcionam como subsidiárias, apenas fazendo parte de uma cadeia produtiva, sem serem notadas pela rede global de forma influente. Todos os processos e normas são definidos pelas empresas mais fortes da rede, sendo que os funcionários da subsidiária apenas são treinados nestes procedimentos para a sua implantação local. A característica mais forte é a influência exercida pelos líderes da cadeia global na empresa, direcionando a forma de atuação e o foco em tipos de produtos e serviços.

Existem também várias empresas nacionais que preferem permanecer focadas em seus mercados locais, possuindo assim uma independência de decisão, porém uma atuação bastante limitada. Estas empresas estão limitadas às fronteiras nacionais, e em alguns casos, atuam apenas nas principais cidades brasileiras. A entrada cada vez maior de empresas estrangeiras no país representa uma ameaça a essas companhias do Tipo C.

As empresas de *software* brasileiras vêm participando deste processo desde a segunda metade da década de 1990, através de parcerias internacionais e, principalmente, com investimentos de grupos empresariais estrangeiros, em alguns casos representando a venda de parte da empresa para estes grupos (SOCIEDADE SOFTEX, 2002).

No capítulo a seguir, vamos descrever resumidamente o mercado de Segurança da Informação no mundo, seus principais líderes e o posicionamento das empresas brasileiras na atuação nacional.

5 O MERCADO DE SEGURANÇA

> Enquanto ocorreram pouquíssimos ataques físicos a CPDs nos últimos 20 anos, os ataques virtuais (*hacking*) e os vírus de computador cresceram dramaticamente (YOURDON, 2002, p. 79).

5.1 Introdução

Este capítulo faz uma análise do mercado mundial de Segurança da Informação, apresentando um breve histórico e algumas tendências em vigor, de forma a situar o leitor nos conceitos relativos às empresas dos estudos de casos, que serão apresentados no capítulo seguinte.

Os últimos anos não têm sido otimistas para o setor de Tecnologia da Informação, não apenas no Brasil, mas em todo o mundo. Yourdon (2002) comenta que os dados disponíveis em 2001 indicam que os atentados de 11 de setembro exacerbaram uma queda na indústria de TI, que já havia começado em meados do ano 2000. Em um curto prazo, esta crise já provocou o adiamento ou cancelamento de vários projetos de TI nas empresas e nas instituições públicas. Apesar disto, Yourdon (2002) rebate estes dados, ao dizer que em longo prazo a TI continuará a ser tão importante como sempre foi, incluindo até mesmo maiores gastos financeiros.

O mercado de segurança é diretamente dependente do bem-estar do mercado de TI como um todo. Na maioria das empresas, os gastos relativos à segurança estão diluídos no orçamento para a área de Tecnologia da Informação. Mas de onde surgiu este "mercado de Segurança da Informação"?

A idéia que se tem hoje a respeito de segurança na área informática é bastante nova. Antes do advento do minicomputador na década de 1970 e do PC na de 1980, a segurança de computadores era pensada em termos físicos (YOURDON, 2002). Basicamente consistia em colocar os *mainframes* em salas bem guardadas, com paredes grossas e com vigias na porta. A miniaturização dos computadores provocou uma mudança de paradigma no campo da segurança de computadores, que cada vez mais deixava de ser física para se tornar lógica.

Proteger o *hardware* dos computadores continua a ter a sua importância, mas os dados armazenados e processados estão muito mais vulneráveis, pois podem ser

alterados, corrompidos, apagados ou copiados, sem os aspectos visíveis da segurança física.

Devido a esta mudança de paradigma, as organizações de todo o mundo vêm focando seus esforços na segurança de seus dados financeiros, médicos, e de propriedade intelectual sobre seus produtos, serviços e clientes.

A segurança de computadores é tão complexa e dinâmica que quase representa uma indústria e uma profissão em si, uma sub-área da ciência da computação. Requer conhecimentos, profissionais e recursos novos. Um pouco destes tópicos será estudado a seguir.

5.2 Segurança da Informação: definições e conceitos

O Glossário de Termos de Telecomunicações (Telecom Glossary 2000, 25 jan. 2004), define Segurança da Informação como sendo "a proteção de informações contra o acesso, transferência, modificação ou destruição não autorizadas, seja acidental ou intencionalmente".

Neste item, apresentamos a Segurança da Informação como uma ciência composta de pilares essenciais, existentes em quase todos os modelos de negócio. Além destes pilares, existem outros aspectos, mais voltados para casos práticos da realidade das empresas, que também serão discutidos. Em seguida, são apresentados os mecanismos mais difundidos para se atender a estes aspectos da segurança. Finalmente, são descritas as principais maneiras de atuação das empresas da área de Segurança da Informação.

5.2.1 Pilares

Os conceitos mais comuns relacionados à Segurança da Informação são os de confidencialidade, integridade e disponibilidade. Existem em todos os livros que tratam deste assunto e podem ser encontrados em qualquer *site* de empresas de segurança. No capítulo 2, vários destes conceitos foram citados nas necessidades de segurança das tecnologias e dos nichos de mercado.

Albuquerque e Ribeiro (2002) caracterizam o termo Segurança da Informação através desses pilares, a saber:

- **Confidencialidade**: conceito relacionado ao acesso a informações confidenciais. A confidencialidade assegura que, em um sistema de informação, apenas

usuários autorizados podem ter acesso a determinadas informações. Para o público geral, podemos dizer que tais informações são ditas confidenciais. Um exemplo é a folha de pagamento dos funcionários de uma empresa. Trata-se de uma informação confidencial, a que apenas um grupo restrito de funcionários possui acesso.

- **Integridade**: está relacionada com a alteração de informações. Um sistema íntegro deve impedir que determinadas informações sejam alteradas por usuários não autorizados, e caso isto venha a ocorrer, o fato deve ser imediatamente detectado pelo sistema. A integridade é um conceito muito importante para transações eletrônicas, tais como saques e transferências bancárias.
- **Disponibilidade**: este pilar diz que determinadas informações de uma empresa, de uma universidade ou de um sistema de informação devem sempre estar disponíveis quando forem requisitadas. Por exemplo, o *site* de uma empresa precisa estar sempre disponível para o acesso dos clientes. Uma única hora em que a página esteja "fora do ar" pode significar um prejuízo de grandes cifras para o negócio.

Quando tratamos de informações, as mesmas costumam apresentar os três pilares descritos acima, com maior ou menor importância, de acordo com o caso específico. A seguir, veremos como estes conceitos são abordados de forma mais próxima aos problemas reais das organizações em geral.

5.2.2 Aspectos

Existem diferentes nomenclaturas para se referir às características da Segurança da Informação. Albuquerque e Ribeiro (2002) citam os seguintes aspectos:

Autenticação: Quando uma pessoa se autentica na vida real, como, por exemplo, para entrar nas dependências de uma empresa ou para realizar uma prova de vestibular, aquela está comprovando ao "sistema" (no caso a empresa ou a instituição de ensino) que ela é de fato quem diz ser. Isto costuma ser feito através de um crachá ou de um documento oficial de identidade. No caso de sistemas de informação, a idéia é a mesma. Para um usuário utilizar determinado sistema, banco de dados ou mesmo acessar uma rede de computadores corporativa, ele precisa se autenticar. Isso pode ser feito através do uso de biometria, por exemplo.

Não-repúdio: O conceito de não-repúdio é bastante conhecido nas instituições sociais. Quando um indivíduo vai ao banco e autoriza a transferência de determinada

quantia de dinheiro para uma outra conta, ele assina alguns papéis em presença do seu gerente de conta. Feito isso, ele não poderá negar posteriormente a realização da operação. O banco possui a prova de que o sujeito, em pessoa, autorizou a transferência, mesmo em caso de argumentação contrária. No "mundo virtual", a analogia é a mesma, porém os mecanismos são diferentes. Não repúdio é um aspecto bastante importante para sistemas de transações financeiras ou de compras pela Internet, e costuma ser suportado por tecnologias de certificação digital.

Legalidade: Este aspecto diz respeito à aderência de um sistema de informação à legislação em vigor. Um exemplo é a aderência obrigatória dos sistemas que participam do SPB (Sistema de Pagamentos Brasileiro, citado no capítulo 2) às normas definidas pelo Banco Central.

Privacidade: Capacidade de um sistema manter incógnito um usuário, impossibilitando a ligação direta da identidade deste com as ações por ele praticadas. Este é um conceito diferente de confidencialidade, e é aplicado no caso de eleições eletrônicas, onde não deve ser possível a associação do voto com o eleitor.

Auditoria: Conceito bastante comum nos dias de hoje. A idéia reside em averiguar que determinado processo está em conformidade com o que foi definido. Em sistemas computacionais, o objetivo da auditoria é verificar todas as ações praticadas pelos usuários no sistema, detectando fraudes ou tentativas de ataque. É claramente um aspecto que vai de encontro à privacidade, e precisa ser balanceado com a mesma.

Tanembaum (1997), de maneira similar, coloca que os processos que garantem a Segurança da Informação se encarregam de:

- Não permitir que pessoas mal-intencionadas leiam ou modifiquem mensagens que não lhes foram destinadas;
- Não permitir que pessoas acessem serviços remotos para os quais elas não foram autorizadas;
- Fazer a distinção de uma mensagem verdadeira de uma falsa;
- Evitar que pessoas neguem o envio de determinada mensagem ou a execução de determinada operação, como, por exemplo, a compra de um livro pela Internet.

Pela categorização de Tanembaum (1997), as questões relacionadas à segurança de redes podem então ser divididas em sigilo, autenticação, não-repudio e controle de integridade. De uma maneira geral, os problemas de segurança se encaixam em um ou mais destes aspectos. Veremos a seguir os mecanismos utilizados para tratá-los.

5.2.3 Mecanismos

Constantemente surgem novas tecnologias para tentar "resolver" os problemas da Segurança da Informação. Como os remédios, elas são vendidas e aplicadas nas empresas, muitas vezes sem a devida "prescrição". Ao invés de descrever as inúmeras tecnologias disponíveis na área de segurança, procuramos aqui agrupá-las nos principais mecanismos utilizados no mercado.

5.2.3.1 Identificação de usuários

Quando acessamos nossa conta bancária através do *Internet Banking*, é exigido o número de identificação da conta corrente e uma senha. Neste momento, estamos nos identificando para o *site* do banco.

Segundo Yourdon (2002), a identificação de usuários diz respeito "a quem" (ou "o que") está tentando acessar algum *hardware*, rede, programas ou dados.

Um mecanismo bastante usado ultimamente é o Gerenciamento de Identidade (LONEEFF, 2003), que visa garantir que o usuário esteja cadastrado em todos os sistemas que ele precisa utilizar, e apenas nestes. Outra tendência são as soluções de *single sign-on*, que vinculam a autorização inicial de autenticação aos sistemas do ambiente, de forma que com uma única senha o usuário tem acesso a tudo aquilo a que ele está autorizado.

As características de segurança atendidas por esse mecanismo são a autenticação e a auditoria.

5.2.3.2 Autorização e controle de acesso

Estes mecanismos se preocupam com "o que" o usuário possui permissão de fazer no sistema, como, por exemplo (YOURDON, 2002):

- Quais redes ou servidores a pessoa está autorizada a acessar?
- Quais programas o usuário está autorizado a usar, operar ou executar?
- Quais dados o usuário está autorizado a acessar, e de que maneira?
- Durante qual período o usuário está autorizado a acessar os vários componentes de *hardware* e *software* no sistema?
- De que localidade e de qual dispositivo de acesso o usuário está autorizado a acessar o sistema?

Os mecanismos mais comuns, segundo Loneeff (2003), são os Sistemas de Autenticação. Estes também utilizam a combinação de *login* e senha, em geral muito

fácil de se "quebrar". Diante deste quadro, as soluções de autenticação forte, geralmente apoiadas por um instrumento físico, têm crescido no mercado. Exemplos: *tokens*, certificados digitais e recursos de biometria, como leitura de íris e de impressões digitais. Youdon (2002) também prevê que técnicas de identificação baseadas em biometria se tornarão a norma no futuro.

Já o controle de acesso de fora para dentro da empresa (e vice versa), é garantido pelo *firewall*, um sistema ou grupo de sistemas que protege a fronteira entre duas ou mais redes. Pode ser comparado à polícia de fronteira de um país, controlando tudo e todos que entram e saem.

As características aqui atendidas são a autenticação, a privacidade e a auditoria.

5.2.3.3 Proteção de dados armazenados

A integridade dos dados armazenados na empresa, seja em bancos de dados, disquetes ou mesmo nas estações de trabalho dos funcionários, é um dos conceitos mais antigos em relação à Segurança da Informação. E nos remete a uma das tecnologias mais conhecidas quando se fala em segurança: os antivírus. Estes são *softwares* capazes de detectar e remover arquivos ou programas nocivos, *e-mails* e demais recursos lógicos dentro da empresa. Os aplicativos antivírus mais comuns baseiam-se em listas, que são atualizadas freqüentemente pelo fabricante, e que contém os últimos vírus surgidos no mundo.

Segundo Loneeff (2003), atualmente é importante que os antivírus sejam distribuídos e proativos, detectando comportamentos estranhos, mesmo que estes não sejam identificados em sua lista de vírus conhecidos.

A principal característica contemplada pela proteção de dados armazenados é a integridade.

5.2.3.4 Proteção de dados em trânsito

A Internet é o meio de transmissão de dados atualmente mais utilizado, e possui uma série de vulnerabilidades. Uma quantidade enorme de dados é transmitida a partir de um local (potencialmente seguro) para outro (também potencialmente seguro), através de várias regiões de um espaço aberto, desprotegido e potencialmente hostil: a Internet. Na medida em que o dado se move de A para B, existe o risco de que o mesmo possa ser bloqueado, excluído, interceptado ou sutilmente alterado (YOURDON, 2002).

A principal tecnologia utilizada para dar segurança à transmissão de dados é a criptografia: codificação de mensagens de forma que sejam ininteligíveis para qualquer pessoa, a não ser para as que possuam a chave requerida para decodificar a mensagem em sua forma original. Atualmente, as tecnologias de criptografia evoluíram para o que se chama de PKI (*Public Key Infrastructure*), um mecanismo, baseado em pares de chaves publicas e privadas, que permite uma melhor administração das chaves utilizadas no processo.

Segundo Loneeff (2003), também são utilizadas VPNs, ou Redes Privadas Virtuais, conexões criptografadas que, normalmente, se estabelecem via Internet em relacionamentos B2B, com o objetivo de proteger os dados em trânsito.

As características aqui atendidas são a integridade e a confidencialidade.

5.2.3.5 Auditoria de acesso às informações

A auditoria é uma prática comum das empresas que lidam com informações financeiras e transações diárias. Os mesmos aspectos valem para a segurança de computadores. Assim como um registro financeiro, um sistema computacional irá manter um registro (também conhecido como *log* ou trilha de auditoria) contendo as atividades e transações relevantes executadas pelos usuários do sistema (YOURDON, 2002).

A auditoria traz à tona o conflito entre segurança e privacidade, já que muitas empresas vasculham registros e *logs* contendo informações sobre *e-mails* e acessos à Internet, com a justificativa de estarem garantindo a segurança da organização.

Loneeff (2003) também cita o Controle de Conteúdo, o qual vincula-se a vários aspectos de respaldo legal, utilização adequada de recursos e desempenho na rede. Segundo o autor, a maior parte dos acessos à pornografia e das transações de Comércio Eletrônico feitas por pessoas físicas são realizadas em horário comercial. Mas os controles mais importantes dizem respeito a *downloads* de *software* pirata; materiais ilegais, como pornografia e pedofilia; e materiais protegidos por direitos autorais, como músicas. Estes *downloads* podem sujeitar a empresa a complicações judiciais, além de consumirem enorme parcela dos recursos de banda dos *links* de comunicação da empresa.

Neste caso, o aspecto atendido é a auditoria.

5.2.3.6 Controle de banda

Este mecanismo está na fronteira entre o gerenciamento de segurança e o de infra-estrutura (Loneeff, 2003). É o caso em que a gestão de segurança contribui para que a empresa deixe de perder dinheiro e garanta a continuidade do negócio. Para isso, é preciso saber o quanto de banda é utilizada para cada serviço e em quais períodos o tráfego deve ser priorizado para quais aplicativos, de forma a obter-se o desempenho desejado. Uma utilização inadequada dos *links* de comunicação pode prejudicar o desempenho de aplicações de missão critica ou mesmo "derrubá-las". Um excesso na utilização da banda pode indicar também que algo estranho esteja acontecendo, como, por exemplo, um ataque externo.

A disponibilidade é o principal aspecto atendido pelo controle de banda.

5.2.3.7 Monitoração de intrusos potenciais

A monitoração é uma estratégia tradicional dos centros de investigação policial, com o objetivo de acompanhar as ações de indivíduos ou grupos suspeitos de atividades ilegais. Segundo Yourdon (2002), no campo da computação a monitoração envolve técnicas específicas de análise de acesso a redes, onde analistas de segurança procuram padrões de acesso suspeitos, de forma a prever ataques ou até mesmo reagir aos mesmos em tempo.

Loneeff (2003) se refere a estes mecanismos como "Detecção de Intrusão". Os sistemas de detecção de intrusos alertam os administradores sobre intrusões reais ou tentadas, inclusive aquelas que o *firewall* não detecta (por exemplo, as que partem de dentro da organização). A base de conhecimento e os algoritmos do produto é que fazem a diferença. Estes sistemas podem ser comparados à polícia e seus investigadores. São sistemas que analisam milhões de linhas de *log* e fazem diagnósticos automáticos. Além disso, também devem ser capazes de identificar um usuário que tente acessar uma aplicação à qual ele não tem autorização ou uma tentativa de quebra de senha.

Neste caso, as características atendidas são a integridade e a confidencialidade.

5.3 Atuação na área de Segurança da Informação

Após esta revisão sobre os principais conceitos da Segurança da Informação, serão discutidas neste item as formas mais comuns de atuação das empresas de segurança.

5.3.1 Desenvolvimento de produtos de segurança

As companhias de segurança mais conhecidas no mundo construíram seus nomes em cima de produtos, na forma de *software* ou *hardware*. A partir do momento em que se identifica uma necessidade para determinado produto, é possível realizar inovações e obter grandes lucros, já que produtos possuem uma escalabilidade muito grande nas vendas. Os produtos de *software* mais comuns e conhecidos são os antivírus e as ferramentas de gerência de identidade. Já os diversos *firewalls* e roteadores, e também os dispositivos de autenticação tais como *tokens* e *smart cards*, costumam vir com *softwares* instalados nos mesmos, que representam *softwares* embarcados, um modelo de negócio que começa cada vez mais a ter importância no mercado de segurança, e que foi discutido no capítulo 3.

Entretanto, como vimos no capítulo 4, a estratégia de se desenvolver produtos requer muitos investimentos em P&D e que as empresas possuam "fôlego" suficiente para aguardar o retorno dos investimentos nas vendas. Particularmente no Brasil, empresas com foco em produtos de segurança são mais raras, devido à dificuldade em se investir em P&D e sobreviver ao mesmo tempo. Empresas prestadoras de serviços e soluções são mais comuns, por trazerem resultados em curto prazo.

5.3.2 Revenda e instalação de produtos

Este é o serviço de segurança mais oferecido pelas empresas de tecnologia em todo o mundo. Praticamente qualquer empresa de TI oferece em seu *site* na Internet algum tipo de serviço relacionado à revenda e instalação. Trata-se exclusivamente de revender produtos (*firewalls*, VPNs, antivírus, sistemas de controle de identidade, dentre outros) desenvolvidos por outras empresas, principalmente multinacionais, e de instalar os mesmos, mantendo contratos de suporte.

Este tipo de abordagem costuma ser conhecido como "segurança periférica", já que os clientes adquirem produtos para proteger a região perimetral de suas empresas. Basicamente toda firma de médio e grande porte, hoje em dia, possui pelos menos um *firewall* instalado, e licenças de algum *software* de antivírus. Trata-se de um mercado de *commodities*, com poucas chances de inovação e já bem explorado.

5.3.3 Serviços Profissionais de Segurança

Essa forma de atuação corresponde a um conjunto de serviços de segurança, em geral serviços de consultoria, que envolve análises e geração de relatórios de conformidade e ação. Os serviços mais comuns são:

Políticas de Segurança

A elaboração de Políticas de Segurança é um tipo de serviço também bastante conhecido mundialmente. Os eventos de 11 de setembro trouxeram à tona a importância de uma política que proteja os ativos informacionais de uma empresa, como bem coloca Yourdon (2002, p. 37):

> Lembram daqueles milhões de pedaços de papéis que estavam flutuando no ar quando as torres desabaram? Muitos destes papéis eram documentos legais à moda antiga – contratos, hipotecas, testamentos – que não foram armazenados em bancos de dados computacionais, porque os documentos possuem valor legal somente em formato físico, com assinaturas de tinta dos indivíduos e entidades relevantes.

De acordo com Puttini (2000), uma Política de Segurança para uma organização deve estar fundamentada em três fatores:

- O que proteger;
- De que proteger;
- Como proteger.

Antes de tudo, é preciso saber **o que** se deve proteger. Uma empresa possui uma quantidade bastante grande de patrimônio físico e informacional, sem contar o patrimônio representado pelas pessoas. Sem uma definição precisa do que deve ser protegido, corre-se o risco de não se dar atenção a patrimônios mais importantes, além de representar um desperdício de dinheiro. Cada elemento a ser protegido dentro de uma empresa costuma ser chamado de "ativo". Exemplos de ativos seriam computadores, documentos, relatórios de vendas e *softwares*. A importância dos ativos, em termos de segurança, varia bastante de empresa para empresa.

Em segundo lugar, é preciso saber **do que** se deve proteger os ativos empresariais. Ou seja, quais tipos de ações podem comprometer os ativos. Existe uma infinidade de maneiras de se invadir o *site* de uma empresa, assim como de obter ilegalmente informações armazenadas em seus servidores internos, ou mesmo de destruí-las. Em outras palavras, a Política de Segurança da empresa deve saber quais são

as ameaças aos seus ativos. Cada ameaça explora uma vulnerabilidade específica do ativo. O mapeamento correto das vulnerabilidades e ameaças aos ativos respectivos é parte vital de uma Política de Segurança organizacional.

O último fator a ser considerado diz respeito a **como** proteger os ativos de suas ameaças. Para isso, procedimentos detalhados do que fazer para minimizar cada ameaça devem ser descritos e seguidos corretamente pelos funcionários da empresa.

O resultado final deste tipo de serviço se resume a uma especificação teórica da Política de Segurança informacional a ser seguida pelos funcionários da empresa, e na prática é implementada com o auxílio de técnicas, *software*, *hardware* e auditoria, ou seja, através dos mecanismos já vistos anteriormente. Tudo isso representa um complexo trabalho de consultoria a ser desempenhado pela própria equipe de TI das empresas ou por consultorias especializadas no assunto.

Análise de vulnerabilidades

Os serviços de análise de vulnerabilidades costumam ser vendidos em conjunto com os de elaboração de Políticas de Segurança. Trata-se de um levantamento de todas as possíveis vulnerabilidades a que estão sujeitos os ativos informacionais da empresa. O produto final costuma ser um relatório, contendo as vulnerabilidades detectadas e as devidas recomendações de correção.

Junto com a análise de vulnerabilidades, costumam ser realizados "testes de invasão". Estes testes consistem em uma bateria de ataques realizada por *hackers*[8] da empresa de segurança, com o objetivo de levantar as possíveis brechas existentes no cliente. Todo o trabalho é feito em comum acordo com os executivos da empresa cliente, e nenhuma informação é de fato roubada ou destruída.

5.3.4 Desenvolvimento de *software* customizado

Diferentemente do desenvolvimento de produtos, neste caso as empresas desenvolvem *software* ou componentes de *software* contratados por clientes específicos, podendo em alguns casos atuar na consultoria para o projeto e desenvolvimento de sistemas seguros. Em geral, podemos citar:

[8] Neste caso, estes profissionais costumam ser conhecidos como *hackers* do bem, pois trabalham para as empresas de segurança e só utilizam seus conhecimentos em testes de invasão.

Desenvolvimento de *software* e componentes de segurança

Como já foi visto no capítulo 3, as empresas brasileiras de segurança costumam possuir modelos de negócio que se encaixam principalmente em **serviços de alto valor**. Estas empresas costumam desenvolver sistemas ou componentes em *software* específicos para atender a determinado cliente. Dependendo da demanda criada, o *software* pode se transformar em um produto a ser vendido para outros clientes, aumentando os ganhos em escala.

Um componente de segurança costuma ser desenvolvido para clientes que também desenvolvem sistemas, mas não possuem conhecimentos de segurança. Por exemplo, pode-se desenvolver componentes que só façam criptografia de dados, ou apenas o envio de *e-mails*.

O desenvolvimento de *software* de segurança é uma tarefa complexa que exige conhecimentos de tecnologias específicas, tais como criptografia, comunicação através de redes, acesso a *hardwares* de segurança, dentre outros.

Segurança no desenvolvimento de *software*

A Segurança da Informação costuma sempre ser percebida em seus aspectos mais visíveis. Estes são contemplados em geral pelas Políticas de Segurança. Entretanto, como já foi dito no capítulo 3, a inteligência de todo o processo computacional está no *software*, e é exatamente nele onde residem os maiores perigos. Yourdon (2002) ressalta a pouca importância dada à segurança no desenvolvimento de *software*:

> [...] é incrível ver o pequeno número de organizações que seguem algum passo para proteger os milhões de linhas de código COBOL, C++ e Java que seus programadores escreveram. O código fonte incorpora as regras de negócio, políticas, estratégias, invenções e segredos de propriedade com os quais o negócio se torna hábil a competir efetivamente; e proteger esta parte de nossa infra-estrutura de TI será também uma parte importante do mundo pós-11 de setembro (YOURDON, 2002, p. 59-60).

Albuquerque e Ribeiro (2002) apresentam um tipo de serviço de segurança conhecido como "Segurança de Desenvolvimento de *Software*". De acordo com os autores, este tipo de serviço envolve três áreas chave:

- Segurança do ambiente de desenvolvimento: relacionada à proteção do código-fonte, para que o mesmo não seja roubado ou mesmo alterado sem autorização;
- Segurança da aplicação desenvolvida: voltada para o desenvolvimento de uma aplicação que implemente corretamente uma série de requisitos de segurança,

livres de códigos obscuros ou maliciosos (*backdoors*) e de falhas que possam comprometer a segurança;

- Garantia de segurança da aplicação: objetiva garantir a segurança da aplicação durante o processo de desenvolvimento.

Estas três áreas são complementares, e não há como tratar da segurança de uma aplicação sem considerá-las no conjunto. No Brasil, o mercado de segurança para o desenvolvimento de *software* ainda é muito pequeno, sendo que a maior parte dos executivos de TI desconhece o assunto. Mas na América do Norte e Europa já existem vários laboratórios e empresas especializadas para atuar e certificar sistemas nesta área.

O conceito básico da Segurança em Desenvolvimento de *Software* está apoiado na norma internacional *Common Criteria*, que se trata de um modelo para a certificação de produtos de TI de acordo com as suas características de segurança. O Brasil ainda não aderiu à norma mundial.

5.3.5 Soluções de segurança integral

Com a queda na procura por implantação de Políticas de Segurança e com a "comoditização" de produtos como *firewall*, as empresas de segurança começam a oferecer soluções integrais para os clientes.

Segundo Loneeff (2003), as melhores metodologias do mercado recomendam o conceito de segurança integral: a combinação de diferentes componentes de segurança que, atuando em conjunto, criam uma barreira defensiva muito mais ampla, eficaz e difícil de ser transposta do que suas atuações em separado.

Esta abordagem "holística" da segurança vem sendo utilizada pelas principais empresas da área, e reúne os outros tipos de atuação descritos anteriormente, oferecendo aos clientes soluções específicas de um mesmo produto ou serviço.

A seguir, daremos uma visão resumida do mercado mundial de segurança, com as principais empresas atuantes.

5.4 O mercado atual de Segurança da Informação

5.4.1 Visão geral

Assim como ocorreu com as Tecnologias da Informação ligadas à Internet, a Segurança da Informação teve o seu período de supervalorização, até o fim do ano de

1999, e em seqüência uma queda acentuada, motivada pelos cortes de gastos nas áreas de TI das empresas.

O mercado de segurança é bastante novo, possuindo algo em torno de dez anos. De uma maneira geral, como foi dito anteriormente, ele começou a tomar força com a proliferação do uso das redes corporativas e, acima de tudo, com a entrada das empresas na Internet. Em um primeiro momento, empresas especializadas em tecnologia de redes passaram a abordar também os problemas de segurança que começavam a surgir. Dessa maneira, tais empresas ofereciam alguns produtos e, mais tarde, serviços de segurança.

Somente quando o mercado viu a grande oportunidade que a segurança de TI representava, é que surgiram empresas especializadas no assunto, ou seja, as empresas da área conhecida como Segurança da Informação. Estas empresas, pouco a pouco, foram se especializando em nichos específicos, tais como os que foram vistos no item anterior.

Um marco mais recente foi a entrada dos grandes nomes do mercado na competição de segurança, tais como IBM® e HP®, oferecendo produtos em *software* e *hardware* e serviços de consultoria. Até mesmo empresas de serviços profissionais, tais como KPMG® e Ernst & Young®, desenvolveram seus serviços de consultoria na área de segurança.

O quadro atual é bastante diverso, sendo que a maioria das empresas acaba promovendo uma atuação genérica na área de segurança, o que na prática nem sempre corresponde à realidade. Com as mudanças drásticas no mercado mundial, desde o início dos anos 1990 até os dias atuais, a estratégia das empresas em todo o mundo sofreu alterações diversas, transformando aquelas em verdadeiras metamorfoses organizacionais (como foi analisado no capítulo 4).

De acordo com o *International Data Corporation* (IDC), o mercado de segurança, englobando *hardware*, *software* e serviços, movimentou US$ 17 bilhões em 2001, e existe uma previsão de que mais de US$ 45 bilhões serão investidos em Segurança da Informação até o ano de 2006 (ROBERTS, 2003).

No item a seguir, será apresentada uma perspectiva do mercado mundial de segurança, a partir de suas principais empresas e suas características marcantes.

5.4.2 Principais empresas

Com o objetivo de apresentar uma noção do mercado de segurança em todo o mundo, são apresentadas neste item as sua empresas mais marcantes até hoje, e as que

possivelmente marcarão o futuro próximo. Para tal, foi utilizada uma análise feita por Briney (2002).

O autor listou as cinco maiores empresas que definiram o mercado de segurança em todo o mundo, de 1997 a 2002, utilizando um critério baseado nos seguintes pontos:

- Total da base de produtos instalada;
- Duração do impacto provocado no mercado pela empresa;
- Utilização de um modelo de negócios de sucesso;
- Desenvolvimento de solução inovadora para um problema de segurança especifico;
- Estabelecimento de padrões mundiais pela empresa.

Na tabela a seguir, apresentamos as cinco empresas mais importantes na área de Segurança da Informação, no período compreendido entre 1997 e 2002, de acordo com o critério descrito acima:

Nome da empresa	**Justificativa**
Check Point *Software* Technologies®	Empresa que popularizou os *firewalls* para mercado empresarial. Mais de 40% de todo o mercado pertence à Check Point®. Além do *firewall*, a **empresa também foi a primeira a inovar com tecnologia VPN, e o** primeiro fornecedor de segurança a vender em uma única caixa o seu *firewall* e sua VPN. Além disso, a empresa foi responsável por criar a plataforma OPSEC® (*Open Platform for Security*), um padrão utilizado por mais de 325 parceiros comerciais.
Internet Security Systems®	A ISS® nasceu da idéia de um estudante de 19 anos, que basicamente era desenvolver uma tecnologia que identificasse, de forma ativa, problemas de segurança de rede, e recomendasse as ações corretivas. Desta idéia, nasceu a primeira ferramenta de busca por vulnerabilidades, voltada para o mercado corporativo, o Internet Scanner®. Em dez anos, a ISS® ajudou a transformar a análise de vulnerabilidades de uma "magia negra de porão" em um componente integral da gerência de riscos empresariais. A ISS® chegou a ser uma empresa de um quarto de bilhão de dólares, com mais de 10.000 clientes corporativos.
RSA Security®	A RSA® foi a empresa que inovou ao criar o algoritmo de chave pública mais utilizado em todo mundo, é a dona do maior mercado de *hardware* de autenticação, e patrocinadora da maior conferência mundial da indústria de segurança. Além disso, grande parte da Internet está construída em cima do algoritmo RSA e de suas licenças. Este algoritmo está entre as maiores inovações técnicas do século XX, e trouxe ao mundo uma solução elegante, como diz Briney (2002), para problemas até então insolúveis: manutenção de autenticação e confidencialidade em sistemas distribuídos e troca segura de chaves de criptografia através de um canal inseguro. A conferência anual promovida pela companhia reúne 12.000 profissionais de segurança.
Network Associates®	**Talvez a maior importância da NAI® tenha sido a sua tentativa de reunir** tecnologias a princípio adversas em uma única suíte de segurança. Mesmo com o mercado não comprando esta idéia, a mesma representou um marco e uma ousadia por parte da direção da empresa, talvez a mais visionária de todas. Atualmente a NAI® não pode ser considerada uma empresa de segurança, mas sim uma empresa que vende um leque de produtos com características de segurança.

Computer Associates®	A CA® foi uma das primeiras empresas a atender à demanda corporativa por aquilo que Briney (2002) chama de "sistemas de gerência holística da segurança empresarial". Desta estratégia, nasceu o eTrust®, uma espécie de ERP composto de módulos focados em aspectos distintos da segurança: gerência de identidades, controle de acesso e tratamento de ameaças.

Tabela 9 – As cinco empresas de segurança mais importantes do mundo no período 1997-2002

Fonte: Elaboração própria, adaptado de Briney (2002).

Para a escolha da lista das empresas que prometem marcar profundamente o mercado de segurança nos próximos cinco anos, Briney (2002) baseou-se nas seguintes características:

- Empresas que oferecem uma única solução ou competência;
- Posição forte de mercado;
- Objetivos bem definidos;
- Grande probabilidade de sucesso.

A tabela a seguir apresenta as empresas escolhidas:

Nome da empresa	Justificativa
Symantec®	A Symantec® lida com aquilo que vem primeiramente à cabeça das pessoas comuns, quando se trata de segurança: vírus, e no caso da empresa, antivírus. Estes fazem parte das ferramentas mais desenvolvidas em todo mundo para o nicho de segurança, e a Symantec®, com 20 anos de existência (não todos voltados para segurança), é a líder em vendas. Atualmente, além dos antivírus, a Symantec® desenvolve um leque de produtos de segurança, para áreas como segurança da *Web*, controle de acesso, gerência de segurança corporativa, serviços de alerta de segurança, monitoração, etc. E a visão da Symantec® para os próximos cinco anos é dominar os mercados de segurança corporativa e pessoal. Para o mercado dos consumidores caseiros (pessoal), a companhia pretende tornar as suas ferramentas de *firewall* e gerência de estação de trabalho tão comuns como os seus antivírus são atualmente.
Microsoft®	Apesar de todas as críticas, é inegável o impacto da Microsoft® na segurança das tecnologias de informação, com a sua histórica ênfase nas funcionalidades às custas do sacrifício da segurança. A influência da empresa irá continuar pelo menos para os próximos dez anos. A Microsoft® costuma alegar que a sua má fama na área de segurança provém da sua grande presença na mídia, e da sua gigante base instalada em todo mundo, o que provoca o foco absoluto de todos os *hackers*. O fato é que muito do que se criou em termos de segurança no mercado foi motivado (positiva ou negativamente) pela gigante do *software*. A nova plataforma .Net®, criada pela companhia, promete revolucionar o conceito de segurança e a forma como as vulnerabilidades vinham até então sendo exploradas.
Cisco Systems®	A nova estratégia da Cisco®, empresa que sempre esteve envolvida com a segurança, graças a seus dispositivos de *hardware* voltados para rede, está focada na segurança baseada em uma arquitetura de voz, vídeo e dados integrados. A Cisco também pretende evoluir a sua estratégia de uma filosofia focada em produtos pontuais para um modelo de processos, com uma visão mais holística.
IBM®/Tivoli®	A presença da IBM® nos próximos cinco anos estará baseada na gerência de identidades (um dos mercados que cresce mais rapidamente na área de segurança), através de um conjunto de *Web services*. Trata-se

	da gerência distribuída de identidades, da habilidade de automatizar os direitos de acesso de usuários às aplicações e recursos de acordo com política pré-definida. A previsão é de que este mercado cresça 30% nos próximos cinco anos.
Tripwire®/Sourcefire®	Estas duas empresas, representadas na tabela como uma só, possuem em comum o seguinte: são pequenas e têm um grande potencial de impacto para os próximos anos. São companhias em que os fundadores tiveram uma grande idéia para uma nova abordagem de detecção de intrusos, e liberaram uma versão *open-source* gratuita de seu *software*. Os *freewares* foram bastante disseminados pelas organizações, mais do que qualquer *Intrusion Detection System* (IDS) famoso, que em geral são muito caros. Nas duas companhias, os fundadores construíram um produto comercial e uma empresa em torno do *software* gratuito. A previsão é de que as duas empresas expandam o seu portifólio de produtos. São empresas baseadas em uma única tecnologia.

Tabela 10 – Perspectiva das cinco empresas de segurança mais importantes no período 2003-2007

Fonte: Elaboração própria, adaptado de Briney (2002).

É importante notar que as empresas escolhidas por Briney, nos dois grupos, são todas norte-americanas (a maioria americanas, algumas canadenses). No quadro de justificativas, é possível identificar uma série de estratégias particulares adotadas por essas empresas, além das estudadas no capítulo 4, tais como o investimento em P&D e o foco em atividades específicas.

Após apresentarmos este quadro mundial do mercado de segurança, veremos a seguir as duas principais tendências de serviços de segurança oferecidos pelas empresas e das necessidades dos clientes.

5.4.3 Terceirização e Gerenciamento Remoto

5.4.3.1 Terceirização de segurança

A terceirização de segurança também faz parte das estratégias de TI. Entretanto, neste caso, os riscos aumentam bastante, e mais cuidados precisam ser tomados. Segurança, integridade e desempenho são alguns dos fatores que devem ser previstos.

Hunt (2001) observa que é preciso ter cautela na terceirização, e coloca que a segurança não pode ser completamente terceirizada. É um conceito que envolve vários processos dentro de uma organização, muitos dos quais devem ser executados pelos donos dos dados e processos de negócios a serem protegidos. A empresa terceira deve se encaixar da melhor maneira possível na cultura organizacional do cliente, fornecendo serviços técnicos que atendam às necessidades. Hunt (2001) ainda sustenta que quanto maior a empresa terceira, menor a chance da mesma satisfazer o cliente: "Empresas grandes não podem sustentar valores personalizáveis" (HUNT, 2001, p. 7).

A perda de confidencialidade é mais relevante no caso das informações estratégicas da empresa. Uma terceirização mal feita pode arruinar a reputação da companhia diante do mercado, a satisfação de seus clientes e a sua capacidade de responder às crises e às oportunidades. Apesar dos riscos, existem vantagens na terceirização dos serviços de Segurança da Informação. Vejamos algumas a seguir.

Vantagens

Conseguir bons profissionais de segurança é uma tarefa bastante difícil, pois os mesmos são raros e caros. As consultorias especializadas em segurança costumam selecionar e manter uma equipe de alto nível, assim como equipamentos necessários, e tornam-se responsáveis não apenas por manter estes equipamentos, como *firewalls*[9], e prevenir ataques, mas também por tomar as providências necessárias quando algum tipo de ataque ocorrer.

Uma outra vantagem desta abordagem é que empresas especializadas em gerência de *firewalls* e detecção de intrusos possuem muitos clientes e, desta forma, contam com uma visão global das ameaças à segurança. Um alerta pode ser disparado a todos os clientes, caso um deles tenha sido atacado.

O corte nos gastos representa a principal vantagem. Os custos associados a *software* e *hardware* de segurança aumentam a cada dia. Muitas empresas podem evitar gastos de capital, deixando que terceiros providenciem os seus próprios recursos tecnológicos. Uma boa equipe especializada em segurança é difícil de se achar, e também de se manter. Devido a isso, o grau de habilidades dos recursos humanos das consultorias de segurança tende a ser um grande apelo à terceirização.

Schneier (2001) afirma que, embora seja possível para as organizações construírem serviços de detecção e resposta para suas redes, isto raramente é justificável em termos de custo. Recrutar bons recursos humanos, em regime de 24 horas por dia e 365 dias por ano, é uma tarefa não só custosa, como praticamente impossível nas

---

[9] De acordo com Schwartz (2001), para companhias que queiram instalar um *firewall in loco*, estes podem custar de US$ 15.000,00 a US$ 30.000,00 ou até mais. Já para instalar um *firewall*, configurá-lo e gerenciar os seus procedimentos de segurança, uma empresa precisaria contratar um profissional especializado, que nos Estados Unidos costuma ganhar entre US$ 80.000,00 e US$ 100.000,00 por ano, além de necessitar de treinamento constante. Os custos de um *firewall* e de mais um único especialista, em um espaço de três anos, não sairiam por menos de US$ 255.000,00. Em contrapartida, utilizar o *firewall* de uma empresa especializada em segurança custa geralmente algo entre US$ 1.000,00 e US$ 3.000,00 mensais, mais as taxas de configuração e administração.

condições atuais de mercado. Evitar que estes recursos "abandonem o barco" é mais difícil ainda.

A seguir apresentamos algumas das principais desvantagens da terceirização na área de segurança.

Desvantagens

Muitas companhias hesitam em terceirizar as atividades de segurança de suas redes internas, com o medo de que suas informações proprietárias caiam nas mãos de pessoas erradas. Dessa forma, preferem terceirizar apenas parte das operações de segurança, particularmente a parte periférica à sua rede interna.

Outros autores são mais radicais e não aconselham a terceirização dos serviços de Segurança da Informação. Tuesday (2001), por exemplo, enfatiza que se deve sempre manter o conhecimento específico ao negócio dentro da companhia. As áreas que podem ser terceirizadas correspondem aos componentes de infra-estrutura, tais como gerência e configuração de *firewall* e serviços de detecção de intrusos.

Um outro perigo existente na terceirização de segurança é que muitas consultorias da área, criadas recentemente e bastante pequenas, estão ganhando o mercado graças à ignorância dos clientes em relação à Segurança da Informação (TUESDAY, 2001). Muitas dessas empresas, se forem atacadas, não serão capazes de dar conta dos serviços de todos os seus clientes.

Também há preocupações em relação aos recursos humanos. Onde as consultorias de segurança recrutam os seus profissionais e com quais critérios? Geralmente as grandes empresas pagam altos salários por seus profissionais técnicos de segurança, os quais trabalham durante o horário normal. Já em relação às empresas de segurança, é difícil saber que tipo de profissional estará integrando as suas equipes, ganhando que tipo de salário e trabalhando sabe-se lá em que regime de horário.

Muitas empresas estão preferindo possuir sua própria equipe interna de segurança, com medo de confiar a terceiros os seus serviços de extremo risco. Outras estão repassando todas as atividades de segurança a consultorias especializadas, ficando apenas com um único profissional interno, conhecido como *Security Officer*.

A discussão a respeito da terceirização nos serviços de segurança está levando a um novo conceito no mercado, os dos grandes provedores de serviços de segurança, baseados nos *Internet Data Centers*. É o que será visto no item a seguir.

5.4.3.2 Provedores de Serviços de Gerenciamento de Segurança

O mercado de segurança no mundo como um todo se encontra em um processo de redefinição, visto que várias estratégias de produtos e serviços se mostraram frustradas. Esta redefinição passa pela revisão de um conceito errôneo tomado pela maioria das empresas: o de que o problema da Segurança da Informação é um problema de tecnologia. Cada vez mais se verifica tratar-se de um problema de pessoas.

Yourdon (2002) coloca que o maior problema atual, relacionado ao mercado de Segurança da Informação, é que muitas companhias e agências governamentais estão comprando serviços de segurança como se estivessem de volta à era dos *mainframes* de 1975. Porém, a ameaça à segurança está nos *softwares*, nas estações de trabalho dos funcionários, nos *e-mails* de *spam*, nos pequenos detalhes. Não é mais possível combater o problema com uma estrutura rígida, hierárquica, e apenas com poder computacional. É preciso flexibilidade e articulação.

Mesmo com décadas de pesquisa e desenvolvimento de centenas de produtos de segurança, a Internet parece ficar cada vez mais perigosa. Schneier (2001) observa que a crescente complexidade da Internet e de suas aplicações e a euforia em se colocar mais e mais serviços e pessoas *on-line*, somado ao desejo de se conectar todas as coisas, contribuem com o aumento da insegurança no mundo digital.

Confiar a segurança de uma organização em produtos é uma tática frágil. Schneier (2001) coloca que de nada adiantam todos os produtos de segurança estarem instalados e configurados, sejam *software* ou *hardware*, no momento em que a empresa é atacada. O que importa é como será feita a defesa. Comparando com os conceitos da segurança física, isto equivale à existência de alarmes e guardas. Na Internet, a idéia é a de prevenção, detecção e resposta.

Além do mais, todo *software* de segurança, como qualquer *software*, possui defeitos (*bugs*), assim como todo *hardware* de segurança pode conter erros de configuração. E nenhum *software* ou *hardware* irá realizar o trabalho de resposta a possíveis ataques. Isso requer pessoal especializado para analisar aquilo que o *software* ou *hardware* apontou como suspeito (SCHNEIER, 2001).

Esta visão discutida acima vem sendo chamada no mercado de segurança pelo nome de Serviços de Gerenciamento de Segurança (*Managed Security Services*, MSS), uma expressão que envolve seis categorias de serviços (HUNT, 2001):

- Consultoria *on-site*: avaliação de riscos de negócio, levantamento de requisitos chave para segurança e desenvolvimento de políticas e processos de segurança;
- Gerenciamento de perímetro de segurança: instalação, configuração e atualização de *firewall*, *VPN*, *hardware* e *software* para detecção de intrusos;
- Revenda de produtos: fornecimento de *hardware* e *software* para uma variedade de áreas de segurança;
- Monitoramento de segurança: monitoramento e interpretação 24/7[10] de eventos importantes de sistemas que ocorrem através da rede, incluindo comportamento não autorizado e ataques de todo tipo;
- Teste de penetração e vulnerabilidade: varreduras isoladas ou freqüentes com o objetivo de descobrir vulnerabilidades no perímetro lógico ou técnico;
- Monitoramento de conformidade: monitoração de *log* de eventos em busca de mudanças no gerenciamento. O objetivo é encontrar administradores fraudulentos, por exemplo.

As empresas que oferecem este tipo de serviço são conhecidas como Provedoras de Serviços de Gerenciamento de Segurança (*Managed Security Services Providers*, MSSP), e se assemelham aos IDCs, citados no item 2.2.2. Apesar de algumas companhias afirmarem possuir uma solução completa de MSS, as categorias de serviços acima excedem a capacidade de uma única firma, colocando em questão a existência "da" empresa de Segurança da Informação, auto-suficiente.

No capítulo a seguir, iremos analisar três empresas cariocas de Segurança da Informação, procurando apresentar a sua colocação no ambiente brasileiro para TI, as suas estratégias de gestão e a sua atuação no mercado de segurança.

[10] Contrato de prestação de serviços em que a empresa contratada se compromete a estar disponível 24 horas de cada um dos sete dias da semana.

6 ESTUDOS DE CASOS

Este capítulo apresenta três estudos de casos realizados na cidade do Rio de Janeiro, com empresas da área de Segurança da Informação, tendo como foco a descrição das estratégias utilizadas por essas empresas, bem como as suas dificuldades e necessidades no cenário competitivo.

O número de empresas usado na análise parece a princípio pequeno, entretanto reflete o mercado de segurança brasileiro, formado por muitas empresas que dizem fazer segurança, e por poucas companhias que de fato atuam na área. O nome de cada empresa foi substituído por codinomes, a saber, Alfa, Beta e Gama, de forma a preservar o anonimato das companhias e suas posições competitivas no mercado.

Marques e Segre (2003, p. 348) observam que o "tamanho cria uma unidade, um todo que torna simples e combinável a complexidade e heterogeneidade não só de uma empresa, mas de todo o processo econômico". Dessa forma, com o objetivo de simplificar a análise e dar um referencial ao leitor, classificamos as empresas Alfa, Beta e Gama como média, pequena e micro, respectivamente, de acordo com o critério do BNDES para o porte das empresas, descrito no capítulo 3 e utilizado na pesquisa realizada pela Sociedade SOFTEX (2002). Como em alguns casos os executivos destas empresas preferiram não revelar o faturamento anual das mesmas, apresentamos o critério adotado e deixamos que eles próprios classificassem suas companhias em relação ao porte.

6.1 Empresa Alfa

Para este estudo de caso, foram entrevistados o Diretor de Tecnologia e a Gerente de Qualidade e Recursos Humanos na empresa Alfa.

6.1.1 Histórico e evolução

Fundada em 1985 com 13 sócios, a Alfa iniciou suas atividades como pioneira no uso e treinamento em Linguagem C, prestando consultoria em teleprocessamento e implantação de informática corporativa nas empresas. Este pioneirismo em se trabalhar

comercialmente com a linguagem C e com o seu treinamento tornou a companhia um referencial em *software* básico[11] no Rio de Janeiro, e posteriormente em todo o Brasil.

No início, os 13 sócios, em uma sala do centro da cidade do Rio de Janeiro, desempenhavam todas as funções da firma, desde serviços de *boy*, passando pela administração financeira, até a complexa tarefa de desenvolver *software* básico. Até mesmo as fases finais de produção, como embalar o *software* e prestar suporte ao usuário final, eram desempenhadas pelos sócios. Com o passar do tempo, a empresa foi conquistando um maior número de clientes, e começou-se a contratar pessoal específico para as tarefas que fugiam ao desenvolvimento de *software*. Nesta época, podemos classificar a Alfa como uma *software house*, desenvolvedora de produto/pacote.

Identificamos o período de 1986-1987 como o primeiro grande marco na história da Alfa. Foi quando se percebeu que a empresa não podia mais ser gerida apenas pelos técnicos, e foi incluído mais um sócio, o único com competências administrativas e de gestão. Enquanto este sócio cuidava da gerência da empresa, os outros eram responsáveis pelos treinamentos, desenvolvimento de *software* e demais serviços que a firma prestava. Nesta época, o número de sócios da Alfa já havia sofrido uma grande redução.

O Diretor de Tecnologia da Alfa também relatou que, no início, todos os fundadores, ainda estudantes, eram os típicos sonhadores, e queriam fazer uma empresa com várias especializações. Nas suas palavras: "Tínhamos até um departamento de inteligência artificial. Acho que as empresas começam assim mesmo, para depois achar sua identidade. Hoje temos uma visão focada".

A partir da década de 1990, foi escolhido como foco de atuação da empresa a área de Segurança da Informação, já que os *softwares* de prateleira então desenvolvidos pela Alfa e de maior sucesso no mercado estavam bastante relacionados à segurança dos microcomputadores. Também nessa época, os diretores da Alfa tentaram se aventurar no mercado externo, deixando de ter como visão apenas o mercado brasileiro, o que representou um segundo grande marco. A experiência, de acordo o Diretor de Tecnologia, não teve muito sucesso, mas serviu como aprendizado para a empresa a respeito do mercado global.

Identificamos o terceiro marco por volta de 1996, quando se resolveu direcionar a Alfa para o mercado de Internet, que começava a demandar muito mais segurança que

---

[11] O termo *software* básico aqui se refere a todo *software* ou componente de *software* que interage com as funções de mais baixo nível do sistema operacional e de protocolos de rede.

o mercado dos microcomputadores. Isso está bem claro no relato do Diretor de Tecnologia: "A gente era essencialmente uma empresa para o mundo dos PCs e, depois desse momento, passamos a ser uma empresa voltada mais para soluções no mundo da Internet".

Com a entrada no mercado de Internet, o entrevistado relatou que se tornou evidente a falta de uma consultoria que suportasse os produtos da empresa. A estratégia foi então modificada, e a Alfa passou a ser uma empresa de soluções de segurança, como foi colocado em uma das entrevistas:

> Nós deixamos de ser apenas uma fábrica de "remédios" e passamos também a ser os "médicos", receitando corretamente o uso do "remédio". Disso surgiu a idéia daquilo que mais tarde viria a ser uma solução integrada e completa de segurança.

Com essa decisão, foram feitos grandes investimentos na área de gestão do conhecimento, e desenvolveu-se uma metodologia própria para a execução de serviços de Segurança da Informação, o que tornou a Alfa uma referência nacional na área de Serviços Profissionais de Segurança.

Em 14 de março de 1997, a empresa obteve o seu primeiro certificado, ISO 9002, tendo sido certificada assim a qualidade da sua metodologia de execução de serviços de segurança. Em 1999, alcançou-se o maior dos certificados ISO série 9000, sendo qualificada como ISO 9001. Das três empresas estudadas neste trabalho, foi a única a obter o selo de qualidade ISO 9001 para as atividades de desenvolvimento de *software* e de consultoria. A partir de então, passou-se a adotar na empresa um modelo de Gestão por Processos, que, segundo a Gerente de Qualidade e RH, teve como principal objetivo "tornar a empresa ágil e flexível, possibilitando a qualquer momento reorganizar rapidamente as peças internas para garantir o atendimento das necessidades do mercado".

Mas o principal marco na história da empresa, na opinião dos entrevistados, foi a entrada de capital de investidores externos, em 1999. Isso fez com que a Alfa ficasse mais profissional e pudesse viabilizar uma série de projetos, entre eles a mudança para um prédio de quatro andares no centro do Rio de Janeiro. Ao todo, a Alfa recebeu dois aportes de capital, sendo que o primeiro teve como fonte várias empresas investidoras e programas governamentais, como a FINEP. O segundo investimento veio em 2001, através de uma multinacional da área de tecnologia, bastante conhecida em todo o mundo, e representou a venda de 40% da Alfa, que deixou então de ser comandada

apenas pelos sócios fundadores. Foi importante notar que este segundo aporte de capital fazia parte de uma estratégia maior da empresa estrangeira, que via a possibilidade do mercado de Segurança da Informação sofrer um "*boom*" em todo o mundo. Possuindo parte de uma empresa brasileira, já conhecida no mercado, a multinacional teria uma porta de entrada já estabelecida no país para a área de segurança.

Ambos os investimentos externos foram bastante necessários para a implantação de uma estratégia ousada: direcionar o foco de atuação da empresa para a integração de serviços e produtos de segurança, em qualquer parte do país. Com esta estratégia, cada vez mais o desenvolvimento de *softwares* de segurança foi deixando de ser uma competência essencial na empresa, sendo substituído pela execução de serviços profissionais.

Com as diversas crises que se sucederam na economia brasileira e mundial, afetando bastante o mercado de Segurança da Informação, a Alfa precisou passar por várias reestruturações, inclusive a redução do número de funcionários e diversos cortes de custos. Apesar disso, ela ainda é, atualmente, uma das principais empresas de Segurança da Informação no Brasil e uma das primeiras no mundo a se voltar exclusivamente para este mercado. Um dos seus marcos de sucesso e reconhecimento foi a coordenação e planejamento da segurança das eleições brasileiras, nos anos de 1994, 1996, 1998, 2000 e 2002.

A companhia tem atualmente 100 funcionários distribuídos na sua sede (Rio de Janeiro) e nas suas filiais (Distrito Federal e São Paulo). Além destes, existe um escritório em San Rafael, Estados Unidos, e parceiros nacionais que marcam a presença da companhia em Belo Horizonte e Nordeste. O faturamento anual da empresa não foi revelado, mas os sócios classificaram a firma como de médio porte.

6.1.2 A empresa no mercado de TI

Por estarem atuando no mercado desde 1985, os empresários da Alfa vêm participando ativamente do desenvolvimento de Tecnologia da Informação no Rio de Janeiro e em todo o Brasil. A maioria dos sócios se conheceu quando eles tinham em média 20 anos de idade, e estudavam Informática na UFRJ. Segundo o Diretor de Tecnologia da empresa, a convivência no meio acadêmico foi de extrema importância, muito mais do que as disciplinas aprendidas e o título recebido no final: "é no ambiente plural da universidade que nós obtemos uma ampla visão do mundo", colocou o entrevistado. Podemos de fato perceber que a cultura local, tanto do ambiente

acadêmico quanto empresarial do Rio de Janeiro teve um grande impacto na trajetória da empresa.

De acordo com o Diretor de Tecnologia, a Alfa, desde sua fundação, já participa de associações e programas de fomento à indústria de *software*. Um destes programas é o RioSoft, que faz parte do Softex, descrito no capítulo 3. O sócio coloca que este programa amadureceu com o tempo, pois estava baseado em uma idéia equivocada a respeito da exportação de *software*:

> O conceito importante atualmente para uma empresa não é exportar, e sim globalizar. Hoje em dia, uma empresa não pode ser do Brasil ou de qualquer outro lugar, ela tem que ser uma multinacional. Por isso nós temos um escritório comercial nos EUA, que não está focado em vendas, mas sim em entender o mercado americano, realizar parcerias e relacionamentos, identificar tendências, etc. Isso nunca nos trouxe uma receita de exportação, mas ajudou a empresa a se posicionar como sendo de classe mundial.

A Alfa também se tornou uma empresa mais profissional graças a esse relacionamento com o RioSoft. Foi através das metodologias do programa que os diretores aprenderam a desenvolver um *business plan*[12] e a se preparar para obter investimentos externos de capital. Atualmente, a Alfa não faz mais uso dos serviços do RioSoft, e o Diretor de Tecnologia justifica isso pelo fato da empresa já estar madura: "estes programas são úteis para as empresas que estão em estágios iniciais".

Uma crítica feita também por este entrevistado foi a de que o Softex, assim como outros programas, nasceram como instituições baseadas totalmente em recursos governamentais. Na visão dele, isso era ruim, pois o governo investia recursos financeiros a fundo perdido nas empresas, como foi colocado:

> Atualmente o Softex está híbrido, e a tendência é que ele caminhe para ser bancado com recursos 100% privados. Quanto mais recursos privados nos programas, mais se exige das empresas coisas como receita, valor agregado, gestão voltada para resultados, etc.

A Alfa foi a única das três empresas pesquisadas a realizar exportação de *software*, sendo que esta exportação foi feita sem nenhum auxílio do programa RioSoft. Através de um parceiro americano, localizado na Flórida, a Alfa vendeu um de seus *softwares* nos Estados Unidos, mas sem atingir grandes margens, e colocou no mercado

---

[12] Termo comum no meio empresarial, que corresponde a um documento contendo o planejamento estratégico da companhia, dividido em metas, objetivos e recursos necessários para atingi-los.

nacional o produto da empresa parceira. A partir do momento em que foi abandonada a estratégia de venda de *software* de prateleira, a parceria também foi encerrada.

Os analistas de sistemas da Alfa desenvolveram internamente uma Metodologia de Desenvolvimento de *Software*, obtendo a certificação ISO 9001 para a mesma, como já citado anteriormente. Esta metodologia envolve todas as fases do desenvolvimento de sistemas, desde a concepção, passando pelo projeto e implementação, até os testes e implantação no cliente.

Apesar da sua importância adquirida ao longo da história da Alfa, a área de *software*, a partir da ênfase cada vez maior na execução de serviços de segurança, deixou de ser independente, sendo que o *software* na empresa passou a ser mais um componente dos serviços vendidos. Nos objetivos estratégicos atuais da Alfa, o *software* deixou de representar um foco de investimento. No caso da participação da empresa em algum projeto que envolva o desenvolvimento de sistemas ou consultoria para tal, é realizada parceria com outras companhias especializadas em *software* de segurança.

Como vimos no item anterior, foram obtidos dois aportes de capital na história da empresa Alfa, sendo que o segundo representou a compra de parte da empresa por uma multinacional. A busca por investimento externo, na visão do Diretor de Tecnologia, foi essencial para os objetivos da empresa, principalmente para aqueles relacionados à globalização. Antes do estouro da bolha das empresas "ponto com", a Alfa pretendia abrir o seu capital na NASDAQ, porém este processo ainda não ocorreu, devido às diversas crises ocorridas na economia. Segundo o entrevistado, a abertura de capital para acionistas externos ainda faz parte dos planos dos sócios e dos novos investidores, mas atualmente existem objetivos mais prioritários a serem atendidos.

A própria abertura de capital da empresa, na visão do Diretor de Tecnologia, é um processo a ser perseguido como essencial, em prol do profissionalismo:

> Com o capital aberto, a empresa fica muito mais profissional e com credibilidade no mercado. A empresa passa a ter muitos donos, e a direção fica sob responsabilidade de um conselho diretor, e não à mercê da vontade de três ou quatro pessoas. O objetivo passa a ser viabilizar a empresa, e não trazer retorno para os donos. Eu e os outros dois sócios principais não podemos mais fazer o que queremos aqui dentro.

Também foi relatado que, neste ponto, a Alfa está alinhada às estratégias das grandes empresas globais, já que no Brasil não existe a tradição das empresas criarem conselhos de administração: "os modelos mais comuns no Brasil são empresas familiares", colocou o entrevistado.

Pelos depoimentos nas entrevistas, foi possível observar que as decisões estratégicas da Alfa estão mais dependentes dos investidores externos, principalmente devido à participação dos mesmos em 40% das ações da empresa. Algumas linhas de produtos e atuação foram descartadas e até mesmo reestruturações na organização foram feitas, devido a essa interferência externa.

A Alfa possui parcerias estratégicas com algumas grandes empresas nacionais e internacionais, que de acordo com o Diretor de Tecnologia visam complementar as soluções da empresa. Além disso, existe uma parceria da empresa com um laboratório de pesquisa ligado à COPPE/UFRJ, para a publicação de artigos nos *sites* das duas instituições.

O Diretor de Tecnologia da Alfa citou a alta carga tributária como uma das principais barreiras ao desenvolvimento das pequenas e médias empresas no Brasil. Segundo ele, as PMEs nacionais deveriam contar com mais vantagens fiscais e de créditos, principalmente quando comparadas com grandes empresas estrangeiras que funcionam no país. Além disso, foi citada a dificuldade na realização de parcerias com outras empresas de segurança e a baixa atuação do governo com o seu poder de compra e fomento da empresa nacional, como foi colocado a seguir:

> Sem dúvida, o poder de compra do governo é uma grande alavanca, e é preciso também fomentar o financiamento para que as soluções brasileiras possam ter competitividade no mercado internacional, com apoio à exportação.

6.1.3 Estratégia e gestão

Das três empresas estudadas, a Alfa foi a que apresentou as características de gestão e estratégia mais sofisticadas. Mas nem sempre foi assim, como nos conta o Diretor de Tecnologia da empresa:

> Fundar uma empresa tendo apenas 20 anos, e sem muita experiência no mercado, não é fácil. Cometemos vários erros, mas também pudemos, graças a isso, experimentar vários modelos de gestão. Com o tempo, os erros foram diminuindo. Sempre fomos, e continuamos a ser, bastante ousados.

Na Alfa, foram desenvolvidos sistemas de gestão internos sem equivalentes no mercado brasileiro, principalmente quando se leva em consideração o tamanho da empresa. Para o desenvolvimento destes sistemas, foram utilizados conceitos de gestão do conhecimento, com base em vários pontos tratados no capítulo 4. Através dessas

aplicações, que estão disponíveis na empresa através da *Intranet* corporativa, os diretores da Alfa possuem o controle da informação para auxiliar a tomada de decisões.

A organização da empresa segue um modelo baseado em processos. Na companhia foram mapeados seis processos chave, chamados macro-processos, subdivididos em processos menores. Para cada processo existe um coordenador (pessoa responsável por acompanhar a execução do processo) e um líder (pessoa que possui competência para executar aquele processo). Os projetos são processos temporários, como, por exemplo, os projetos de consultoria realizados nos clientes. Apesar dessa gestão por processos, foi possível perceber na Alfa uma hierarquia, onde estão distribuídos os sócios diretores, os gerentes executivos, os analistas e demais funcionários.

Como já foi citado, existe na Alfa um planejamento de negócios (*business plan*), revisto periodicamente e que contém todos os macro-processos da empresa e os objetivos estratégicos. Segundo a Gerente de Qualidade e RH, este planejamento foi crucial para a captação externa de capital, e tem facilitado bastante as mudanças freqüentes que a companhia precisa realizar perante os acontecimentos do mercado.

A Alfa é uma empresa bastante flexível. A companhia já chegou a funcionar com uma média de 300 funcionários em um único andar do centro do Rio de Janeiro, tendo de alocar alguns deles até mesmo no corredor. A carga horária não é rígida, e as pessoas trabalham por resultados, não sendo cobradas por horas trabalhadas.

A rotatividade da mão-de-obra na Alfa normalmente é baixa, excetuando períodos em que surge grande quantidade de novos projetos, e uma contratação em massa se faz necessária, ou até mesmo a situação (trágica) inversa. A empresa enfrentou, por exemplo, uma redução no segundo semestre de 2000, pois uma série de projetos que haviam sido previstos não se concretizou, devido à crise da NASDAQ, em 1999. Os investidores começaram a exigir lucratividade e, portanto, foi necessário o enxugamento da folha em um número razoável de pessoas.

O processo mais sofisticado existente na Alfa, e que representa uma grande inovação, é o de Recrutamento de Funcionários. Existe na companhia um *software* de recrutamento, conhecido como *Web Hunter*, que permite uma interface com os possíveis candidatos a trabalhar na empresa, através de uma página na Internet. Dessa forma, um banco de dados na empresa vai sendo constantemente alimentado com as informações sobre candidatos. Quando surge uma nova oportunidade em alguma área da

empresa, o *Web Hunter* é então utilizado para buscas, como coloca a Gerente de Qualidade e RH:

> O sistema permite a busca por palavras-chave, permite várias combinações (faixa salarial, universidade cursada, etc.). Este é o primeiro filtro. O *e-mail* do candidato já está disponível no banco, é só "clicar" e enviar um chamado para entrevista ou prova.

A idéia inicial do *Web Hunter* era formar as bases do que viria a ser futuramente o mapa de competências da empresa. Mas por enquanto, trata-se apenas de um banco de dados de currículos. Uma das principais vantagens, segundo a entrevistada, é a facilidade em gerenciar a informação sobre recursos humanos: "eliminamos o papel deste processo completamente".

A Alfa também premia financeiramente os funcionários que indicam outras pessoas, as quais são futuramente efetivadas na companhia. Segundo a Gerente de Qualidade e RH, é uma forma de explorar a rede de contatos dos bons profissionais.

Além do sistema de busca por recursos humanos, também existe um processo bem definido para a seleção das pessoas, o qual envolve a realização de entrevistas pelo RH da empresa, algumas provas técnicas, uma prova de liderança de projetos, uma prova de redação e, se aplicável, uma prova de inglês.

Cada cargo dentro da Alfa possui uma descrição específica, na qual funções genéricas são mapeadas pela diretoria. Logo, quando uma solicitação de pessoal é feita para determinado cargo, já se sabe exatamente qual o tipo de profissional se está procurando.

A Alfa possui, segundo a Gerente de Qualidade e RH, três tipos de contrato de trabalho com os seus funcionários: CLT, cooperativa de trabalho e prestação de serviços. Com a entrada de investidores nacionais e principalmente estrangeiros, a empresa chegou a transformar 75% da sua folha de pagamentos em CLT, enquanto o restante dos funcionários continuava sob os demais regimes. Os investidores foram os principais pivôs dessa mudança, já que por exigência dos mesmos, auditorias eram realizadas constantemente, obrigando a companhia a estar conforme com as questões trabalhistas. Apesar disso, a sucessão de diversas crises financeiras levou a novas reestruturações na empresa em termos de recursos humanos, fazendo com que a maioria dos profissionais que ganhavam altos salários passasse a trabalhar como prestador de serviço.

Um outro ponto forte nas estratégias da Alfa diz respeito à aprendizagem organizacional. Assim que um candidato a uma vaga na empresa é aprovado, ele automaticamente está inserido no processo de Aprendizagem Organizacional e Individual. Qualquer novo funcionário precisa necessariamente passar, após sua contratação, pelos treinamentos específicos da sua função. A empresa possui uma espécie de centro de educação, um departamento voltado exclusivamente para a aprendizagem. Neste centro, existem treinamentos específicos para cada cargo e função dentro da empresa, treinamentos estes que precisam ser realizados periodicamente pelos funcionários. Já existe uma biblioteca com todo o material disponível (o que data desde o início da empresa, em 1985).

Todo o conhecimento obtido fora da empresa é materializado e disseminado internamente. Existe uma base de conhecimentos (*knowledge base)* interna com todas as informações disponíveis na firma sobre questões de Segurança da Informação ou relacionadas. A metodologia de execução de serviços de segurança da companhia é passível de ser replicada e massificada, de forma que cada vez menos se depende do conhecimento de um único indivíduo. Listas de discussão internas também são bastante utilizadas para a disseminação de informações.

A Alfa é uma das poucas empresas no Brasil, segundo a Gerente de Qualidade e RH, a implementar parte de um modelo de gestão por competências. A primeira parte do que a empresa chama de Mapa de Competências já foi implementada: as competências comportamentais. Isto foi realizado através de entrevistas com executivos e com profissionais por estes indicados, tentando se identificar quais eram os comportamentos esperados de cada pessoa dentro da organização. As competências ditas técnicas ainda não estão totalmente definidas, mas existe um trabalho para isso em andamento. Foram escolhidas doze competências, por parte da diretoria, as quais representassem o que a empresa esperava de cada um de seus funcionários. Estas competências resumem um roteiro do que cada funcionário deve desenvolver, como por exemplo, "visão estratégica", "liderança" e "relacionamento interpessoal", e também servem para fins de avaliação.

A Alfa possui uma área de qualidade bastante profissional, empregando conceitos de melhoria contínua e a realização de auditorias internas constantemente. Também existe um projeto de avaliação da satisfação de clientes, realizado mensalmente. Uma consultoria externa entra em contato com os clientes da companhia, questionando-os em relação a itens especificados pela própria Alfa. São gerados

relatórios de satisfação e insatisfação, e estes relatórios são acompanhados pela área de qualidade.

Um outro ponto forte é a área de pesquisa em Segurança da Informação, encarregada de buscar as mais recentes tecnologias de segurança, incluindo as últimas vulnerabilidades descobertas na comunidade mundial. Este mini centro de pesquisas possui laboratórios com equipamentos específicos para testes de tecnologias de segurança. Atualmente, não se investe mais em pesquisa e desenvolvimento na área de *software* na Alfa.

A Alfa possui as áreas de *marketing* e comercial mais fortes das três empresas pesquisadas. O departamento de *marketing* é responsável pela notável presença da empresa nos meios de comunicação e nos diversos eventos de tecnologia no país. Existe um portal de Internet voltado exclusivamente para Segurança da Informação, desenvolvido e mantido pela empresa. Entretanto, pode-se observar que a maior força do *marketing* na Alfa está na figura do Presidente da empresa, um dos executivos de TI mais conhecidos no Brasil, e que realiza palestras em empresas, universidades e instituições do governo.

A área comercial da Alfa está dividida entre as filiais do Rio, São Paulo e Brasília, e conta com profissionais de longa experiência no mercado. Esta área comercial possui muitos contatos no governo e setor privado de TI brasileiro, garantindo à Alfa muitos projetos na área de segurança. Foi possível observar que a filial de Brasília possui a maior força comercial, tanto em número de funcionários como em quantidade de recursos financeiros. Isso se deve à importância do setor governamental na estratégia comercial da empresa.

Na visão do Diretor de Tecnologia da Alfa, a empresa é altamente inovadora. Em suas palavras:

> Poucas vezes nós criamos produtos que já existiam no mercado. Nossas soluções estão quase sempre livres de similares, desde a origem da empresa até hoje. E mesmo quando fazemos algo que já existe no mercado, isso vem com uma abordagem diferente para o problema. Até mesmo a nossa metodologia de execução de serviços foi totalmente inovadora, já que não existia nenhuma ainda no mercado. Tudo que fizemos foi a partir do zero.

Observamos, nas entrevistas e em conversas com pessoas da área de projetos da empresa, que uma das principais inovações na companhia, além do processo de RH, está justamente no desenvolvimento desta metodologia própria de execução de serviços de segurança. Com ela, segundo o entrevistado acima, a empresa materializou os

conhecimentos de execução de projetos de segurança de forma que a tarefa ficasse o máximo possível independente das pessoas. Para aumentar o número de projetos realizados, bastava contratar novos funcionários, colocar os mesmos dentro do processo de aprendizagem da metodologia, e executar as atividades.

Foram adotadas estratégias de terceirização na Alfa, eliminando produtos sem margem de contribuição (antigos *softwares*) e atividades que evidentemente não faziam parte do negócio da empresa, como segurança predial, limpeza e projeto da *homepage* corporativa. Como foi citado anteriormente, a atividade de desenvolvimento de *software* não faz mais parte do foco de atuação da companhia, e seus diretores estão realizando parcerias com outras empresas para cobrir esta competência.

De acordo com o Diretor de Tecnologia da Alfa, uma das principais estratégias aprendidas por eles foi o foco em áreas específicas, e que isso se deveu ao aprendizado com sucessivos erros cometidos: "se pudéssemos recomeçar a história da empresa, teríamos sido mais focados desde o começo", completa ele.

6.1.4 Atuação no mercado de segurança

O discurso de atuação da Alfa vem mudando bastante com o tempo, até mesmo pelo fato da empresa já possuir 18 anos de existência. A atuação inicial no mercado, como já exposto, estava focada principalmente no desenvolvimento de sistemas. A primeira incursão na área de segurança, segundo um dos sócios da Alfa, foi o desenvolvimento de um *software* de proteção contra pirataria de aplicativos.

Outro fator importante que marcou o início de atuação da Alfa foi a sua origem no ambiente acadêmico da UFRJ. O Diretor de Tecnologia lembra que o primeiro Unix instalado no Brasil estava justamente nessa universidade, fazendo com que os estudantes tivessem contato com um sistema de alto nível de segurança. Com a popularização dos microcomputadores nas empresas, os sócios da Alfa perceberam que faltava a estes novos sistemas as características sofisticadas de controle de acesso do Unix, e tiveram então a idéia de desenvolver um *software* que trouxesse esta segurança aos novos equipamentos. Este aplicativo ganhou vários prêmios e teve mais de 100 mil cópias vendidas.

Consideramos que o modelo de negócios para desenvolvimento de *software* da empresa, com base na classificação proposta pela Sociedade SOFTEX (2002), era o de produto/pacote, nesta fase inicial em que a empresa se apresentava ao mercado como uma *software house*. Com a evolução do mercado, os sócios passaram a agregar

serviços à implementação do *software*, passando a vender uma solução para um problema, e não mais apenas uma caixa preta. A companhia passou então a ser uma *software house* que agregava serviço ao seu produto.

O desenvolvimento da metodologia de execução de serviços de segurança, que envolvia não só o desenvolvimento de *software*, mas também a Política de Segurança e outros serviços agregados, transformou a empresa, com o tempo, em uma consultoria especializada em Segurança da Informação. O Diretor de Tecnologia da Alfa ressalta a entrada significativa do governo como cliente, o qual é bastante exigente e interessado em questões de segurança. Com a entrada deste cliente, a empresa precisou refazer sua estratégia para fornecer uma consultoria completa em Segurança da Informação - o que era exigido pelo governo - e não apenas um produto de prateleira.

Com essa metodologia, a Alfa veio praticamente a dominar o mercado brasileiro de Serviços Profissionais de Segurança da Informação, com a implantação de Políticas de Segurança, execução de Análises de Vulnerabilidade e desenvolvimento de soluções customizadas em *software* para os clientes. É importante ressaltar que, com isso, a Alfa deixava de ser uma empresa de *software*, sendo este último apenas um componente da sua metodologia de execução de serviços, e passava a desenvolver serviços de Alto Valor, de acordo com a classificação da Sociedade SOFTEX (2002).

Além dos serviços profissionais de segurança mais comuns, a Alfa foi pioneira em introduzir no Brasil a aplicação da norma internacional *Common Criteria*, para segurança de produtos de TI. Um dos serviços que a empresa oferece é a Análise de Segurança de Aplicações, com o objetivo de dar consultoria a empresas que queiram desenvolver *software* seguro, de uma forma segura, como visto no item 5.3.4.

Por muito tempo a Alfa se manteve líder no mercado de segurança brasileiro, inclusive fazendo frente aos concorrentes internacionais. Com o aumento dos impactos da globalização e a ocorrência de uma série de crises, a companhia foi gradativamente eliminando vários produtos e serviços, como, por exemplo, o desenvolvimento de *software*, focando-se na sua competência essencial: a integração de tecnologia de segurança. Como uma integradora, a Alfa podia então terceirizar todos as atividades não essenciais, e usar a sua experiência em projetos de segurança atuando apenas na integração da solução final. Essa forma de atuar, como uma provedora de soluções integrais de segurança, pode ser comparada ao tipo de atuação descrito no item 5.3.5, e de acordo com o Diretor de Tecnologia, foi introduzida no Brasil pela Alfa:

> Hoje poucas empresas no Brasil oferecem um serviço completo como o nosso. Nós criamos essas soluções integrais de segurança e nos posicionamos assim no mercado há bastante tempo, e só agora começam a surgir nos EUA algumas empresas com essa proposta, de oferecer uma solução completa e integrada de segurança.

Para o sócio, a Alfa é uma empresa da "velha-guarda" da segurança, já que a maioria das concorrentes que hoje atuam no Brasil possui no máximo quatro anos de existência, e ainda está focada apenas nas tecnologias, nos "remédios", como ele coloca. Essas empresas ainda precisariam passar pela fase de descobrir que necessitam se transformar em provedores de soluções completas. O entrevistado colocou o seguinte a este respeito:

> Hoje as empresas precisam ter uma visão corporativa de segurança. A Internet interligou todos os sistemas computacionais, e não é mais possível tratá-los em separado. Para se ter um alto nível de segurança é necessário integrar todos os processo da firma, tanto os computacionais quanto os pessoais.

Outra importante frente é a venda de treinamentos a seus clientes. Existe, por exemplo, um curso para preparação e certificação de *Security Officers*, com o intuito de formar profissionais de Segurança da Informação. Também são vendidos para grandes empresas treinamentos e processos de conscientização em Segurança da Informação.

Os principais clientes da Alfa estão no segmento governamental. As áreas comercial e *marketing* da empresa, como citado no item anterior, sempre foram bastante fortes, e criaram uma importante presença no Governo. Além destes clientes, a empresa também possui negócios realizados com grandes empresas privadas, e segundo o Diretor de Tecnologia, a empresa sempre investiu no que ele chamou de *key accounts*, que são um grupo de clientes de grande porte.

Os concorrentes atuais da Alfa são as grandes consultorias e prestadoras de Serviços Profissionais de Segurança, do tipo Price Waterhouse®, HP® e Unysis®. A Alfa, segundo um dos sócios, absorveu a equipe de segurança de uma multinacional da área de consultoria em TI no Brasil. Os sócios da Alfa não citaram as empresas brasileiras de segurança, tais como a Beta e a Gama, como concorrentes, e sim como parceiras, apesar de que pouca ou quase nenhuma parceria com estas empresas tem sido realizada.

De acordo com informações disponíveis no *site* corporativo da empresa, os diretores da Alfa estão em busca de parceiros em todo o país, para a execução de

serviços que complementem as soluções de segurança oferecidas. Além disso, procuram por parceiros que estejam interessados em executar os serviços da Alfa, usando a sua base de conhecimentos e sua metodologia de execução de serviços. Mas, como já foi citado, o Diretor de Tecnologia da empresa destacou bastante a dificuldade na realização de parcerias, o que ele considera como uma deficiência estratégica das empresas brasileiras de segurança:

> Existe uma grande confusão na oferta das empresas. Parece que todos querem fazer tudo. É preciso maior especialização e foco, possibilitando inclusive maior cooperação e parceria entre as empresas. No Brasil, o mercado de segurança ainda é muito pulverizado e as empresas precisam se aproximar para aumentar a sinergia de atuação. Existe grande potencial de desenvolvimento, mas os esforços são diluídos, repetidos e muitas vezes com grande competição entre as empresas. É preciso fomentar as parcerias e maior cooperação.

Os entrevistados vêem a terceirização da segurança como uma tendência cada vez mais forte. O Diretor de Tecnologia da Alfa acredita no crescimento do mercado, mas com foco na integração de serviços e produtos:

> O mercado de segurança continua em grande expansão, sendo que os principais investimentos dos clientes têm se direcionado para a formação de equipes internas responsáveis por segurança, o que tende a diminuir o mercado de consultoria. Percebe-se também a necessidade de apoiar estas equipes com capacitação e ferramentas adequadas.

A figura a seguir resume a evolução da Alfa ao longo da sua história, com base nas estratégias de atuação no mercado de Segurança da Informação apresentadas no item 5.3:

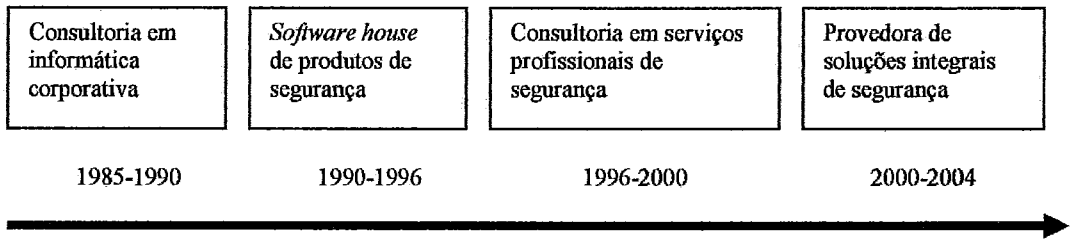


Figura 1 – Histórico de atuação da empresa Alfa.

Fonte: elaboração própria.

6.2 Empresa Beta

Para este estudo de caso, foram entrevistados o Presidente e o Diretor de Tecnologia da empresa Beta.

6.2.1 Histórico e evolução

A empresa Beta foi criada em setembro de 1998 por três sócios, que trabalhavam em grandes empresas de TI na área de vendas e *marketing*. Para cobrir as competências técnicas ausentes, estes sócios convidaram mais três pessoas com maior experiência técnica passada.

Os seis sócios iniciais começaram realizando projetos de consultoria com determinados clientes que conheciam, e somente no final do ano de 1998, todos os sócios puderam se fixar na empresa de vez. Esta foi uma fase de definição das pessoas que realmente fariam parte da empresa, com várias entradas e saídas de sócios. Durante três meses, a Beta foi sendo administrada de maneira informal no Rio de Janeiro, e com um sócio consultor em São Paulo. Em setembro de 1999, a empresa foi legalizada, e junto com os donos, havia uma secretária e mais três analistas de rede, que vieram junto com os sócios mais técnicos.

Segundo o Presidente da empresa, a idéia inicial era trabalhar com serviços relativos a Internet, segurança e Comércio Eletrônico. Pode-se ver aqui uma falta de foco e planejamento estratégico inicial, assim como ocorreu com a empresa Alfa. Nas palavras do Presidente: "Nenhuma empresa nascia, pelo menos naquela época, com essa competência de planejamento, já definindo uma missão, uma visão, etc. É um processo que vai amadurecendo com o tempo".

Dessa forma, o primeiro grande marco na história da Beta, na opinião do entrevistado, foi a escolha por um foco de atuação. Como já existiam projetos sendo feitos na área de segurança de redes, a empresa foi se interessando mais em desenvolver esta competência de atuação. O Diretor de Tecnologia da Beta coloca que, já no início, as competências técnicas dos sócios e funcionários estavam mais voltadas para redes e segurança (instalação e configuração de *firewall* e VPN e estruturação de redes) do que para desenvolvimento de *sites* e Comércio Eletrônico propriamente dito. No final de 1999, foi contratado um consultor em estratégias de negócios, que apontou imediatamente a existência de dois focos de atuação, o que era inviável para a empresa. Após a realização de várias reuniões, a maioria dos sócios optou pela área de Segurança

da Informação. Um dos sócios que mais defendia a atuação na área de Comércio Eletrônico acabou deixando a empresa.

De acordo com o Presidente da Beta, eles abandonaram a parte relativa ao Comércio Eletrônico, no final de 1999, também pelo fato desta área envolver conhecimentos de desenvolvimento de *software*, de banco de dados e de outras tecnologias que os sócios iniciais não conheciam ou dominavam. E já havia muitas empresas trabalhando com Comércio Eletrônico e Internet.

A segunda grande mudança foi a realização de um planejamento estratégico, em meados de 2000. Em grande parte, essa decisão veio no momento em que várias empresas de Internet estavam recebendo aportes de capital de investidores de risco, o que também interessava aos sócios da Beta. Através de um *business plan*, a empresa definiu oficialmente a sua competência básica, que estava mais voltada para a segurança de redes, e não para Internet de uma maneira geral.

Os executivos da Beta planejavam ocupar o segundo lugar na liderança do mercado de Segurança da Informação no Brasil. Segundo o Presidente da empresa, o primeiro lugar já estava claramente dominado pela empresa Alfa, mas a segunda posição estava "disponível". Dessa forma, eles optaram por desenvolver as mesmas competências da empresa concorrente. Tinha-se também a idéia de se estabelecer primeiramente no mercado brasileiro, para depois expandir a atuação para América Latina e até mesmo o mundo. O próprio nome da empresa foi escolhido de forma a ser facilmente aceito em qualquer parte do planeta, como relatou o Presidente.

O terceiro marco de grande importância na história da empresa foi a entrada do aporte de capital, em 2001, conseguido através de um grupo de investidores em conjunto com o BNDES. Com ele, foi possível a mudança para um escritório maior, a compra de equipamentos e a viabilização de diversos projetos que os sócios tinham em mente.

A quarta mudança de grande importância, ocorrida em 2002, e que segundo o Diretor de Tecnologia representou uma reviravolta na história da empresa, foi a participação no projeto do SPB (Sistema de Pagamentos Brasileiro). Isso fez com que se criasse na Beta, pela primeira vez, uma equipe de desenvolvimento de *software*, até então uma área desconhecida dos sócios fundadores. Além disso, marcou a entrada da Beta no mercado financeiro, que, segundo o sócio entrevistado, é formado por clientes bastante reticentes às novas empresas e pragmáticos nas suas decisões de tecnologia.

O quinto grande marco ocorreu no final de 2002, quando a empresa decidiu abandonar a sua atuação na área de *commodities* de segurança (revenda e instalação de *softwares* e *hardwares* de segurança) e tomar um rumo exclusivo na área de desenvolvimento de novos produtos da própria empresa. Segundo o Presidente da Beta, não mais se vendia grandes somas na área de *commodities*, e eles queriam ganhar um mercado mais lucrativo e escalável.

O último grande marco na história da Beta está sendo a sua atual mudança de foco para o mercado de São Paulo, com a transferência de toda a área comercial e gerencial da empresa para a maior cidade brasileira. Segundo o Presidente da companhia, esta mudança se deve a diversos fatores, dentre eles o grande número de clientes que estão no mercado financeiro e que possuem sua base em São Paulo, e a um certo preconceito do empresariado paulistano em relação às empresas cariocas. A Beta já considerou no passado até a possibilidade de mudar a razão social da empresa para São Paulo por questões de *marketing*. Apesar da mudança, a área de *software* da empresa irá permanecer no Rio de Janeiro.

A Beta está em busca de um novo aporte de capital, que pode ocorrer no futuro, através de investidores e empresas multinacionais. A empresa possui atualmente 28 funcionários, e obteve um faturamento de R$ 4 milhões no ano de 2002, podendo ser classificada como uma firma de pequeno porte. Segundo os dois entrevistados, o novo aporte de capital é considerado essencial para o futuro da empresa, que se encontra em uma grave crise financeira.

6.2.2 A empresa no mercado de TI

Na visão dos executivos da Beta, o mercado de Tecnologia da Informação no Brasil ainda está dominado por empresas multinacionais. Em geral, eles apontam que as empresas que mais sobrevivem são as que trabalham com revendas de produtos de multinacionais e que, ao crescerem, conseguem se tornar integradoras. Além disso, destacam a importância das empresas que encontraram o sucesso em nichos específicos, como o de segurança.

O Diretor de Tecnologia da Beta coloca ainda que o mercado de TI no Brasil está cada vez mais se concentrando em São Paulo, como já foi comentado no item anterior. A mudança de empresas, que antes estavam localizadas na cidade do Rio de Janeiro, para São Paulo tem gerado um efeito em cascata, fazendo com que os fornecedores também sejam obrigados a se mudar.

No caso da Beta, os sócios fundadores não se conheceram no ambiente acadêmico, e por isso não vêem grande vantagem na importância da vivência acadêmica na criação de uma cultura tecnológica local. Apesar disso, pode-se observar dois grupos diferentes de profissionais na Beta: os sócios fundadores, mais voltados para a parte de tecnologia de redes, e os novos analistas de sistemas, profissionais da área de pesquisa e desenvolvimento de *software* e que são conhecidos de longa data do ambiente acadêmico, valorizando mais esse tipo de cultura.

Dentro dos objetivos estratégicos da Beta, o *software* é fundamental, como relatou o Presidente da empresa. Para ele, o Brasil possui recursos humanos de excelente qualidade para atuar no desenvolvimento de sistemas. Além disso, conta com uma mão-de-obra relativamente barata, e que poderia competir mundialmente. A empresa tem um departamento de pesquisa e desenvolvimento, formado pelos analistas de sistemas citados no parágrafo anterior. Existe um processo formal de desenvolvimento de *software* criado pelos próprios analistas, mas não certificado.

As certificações na área de qualidade de *software* são vista como essenciais para a empresa. Os sócios se mostraram cientes de que precisarão da certificação CMM para exportar, e isso está no plano de negócios da empresa; estão apenas faltando os recursos financeiros.

A Beta nunca exportou nenhum de seus produtos, mas possui este interesse. Segundo o Presidente da empresa, exportar não é uma coisa simples, e requer a criação de toda uma infra-estrutura para tal. Os seus produtos, na sua opinião, possuem grande potencial de exportação, por se tratarem de tecnologias mais difundidas no exterior do que no Brasil. É o caso dos produtos voltados para certificação digital e assinatura de documentos eletrônicos.

O Presidente da Beta colocou que o governo precisa criar políticas corretas para o setor de informática, com investimentos e incentivos fiscais. "Cobrar mais impostos de quem tem mais, e menos de quem está começando", em suas palavras. Como estratégia positiva, foi citado o aparecimento das incubadoras de empresas. Já em relação aos projetos de fomento à indústria de *software* nacional, como o PROSOFT, do qual a Beta chegou a participar, foram feitas várias críticas. Apesar de considerarem a idéia do programa positiva, a forma como o mesmo é executado não satisfaz à empresa. Como colocou o Diretor de Tecnologia da Beta:

> A cultura de financiamento no Brasil é totalmente invertida. Empresta-se dinheiro para quem não precisa, para quem está com todas as contas pagas,

> etc. Só quem consegue crédito com o BNDES, por exemplo, são empresas como a AES, multinacional, que comprou a ELETROPAULO. Achamos ótima a idéia desses programas de fomento, só que não funciona, pois quem precisa do dinheiro não consegue. Além disso, o PROSOFT foi muito pouco efetivo, já que investiu em apenas quinze empresas durante cinco anos.

Também foi citada a quantidade de requisitos exigidos pelo governo para que as empresas possam participar de programas de fomento. Isso, segundo o Diretor de Tecnologia, é fruto do medo e da desconfiança de que os empresários irão usar o dinheiro para interesses próprios, e não para investir nas empresas, o que leva à criação de vários controles. Porém, esses requisitos acabam por excluir pequenas e médias empresas, que possuem grande potencial para exportação, como foi colocado na entrevista:

> Eu vejo que a Beta tem tudo para exportar. Mas, em primeiro lugar, a gente tem que sobreviver, em segundo tem que se preparar, em termos de estrutura, para sermos capazes de realizar exportações, e para um mercado que possa absorver um pouco do que a gente faz, e em terceiro, precisamos de alguém para nos ajudar a aparecer lá fora. Infelizmente eu percebo que esse tipo de coisa não está sendo vista de maneira estratégica por nossos governantes.

Um outro problema relatado, a respeito da dificuldade para se exportar, é que atualmente as empresas estrangeiras não estão se interessando pelo Brasil. O Diretor de Tecnologia da Beta culpa o governo, por não ter uma política efetiva para levar a marca da tecnologia brasileira para o exterior. E ainda comenta que muitas empresas estrangeiras se surpreendem quando descobrem o potencial nacional:

> Duas empresas estrangeiras, fabricantes de *smart cards*, se espantaram ao ver que existia no Brasil uma empresa que entendia de PKI e certificação digital, e muito mais ainda por existirem por aqui produtos em *software* que trabalham com essas tecnologias.

Para os sócios da Beta, o governo brasileiro deveria desenvolver um programa de promoção do *software* nacional no exterior, com investimento em *marketing*, com linhas de financiamento para compra de ferramentas CASE, treinamentos e certificação em CMM.

Como já foi visto, a Beta cogitou pela primeira vez na sua história a captação de investimento externo quanto passou por sua primeira crise financeira. Segundo o Diretor de Tecnologia, está sendo cogitada uma nova forma de investimento vinda de empresa estrangeira, que teria interesse em produtos da Beta, já que as multinacionais não estão

mais interessadas em investir em uma empresa brasileira de segurança. Nas suas palavras:

> Eles estão agora interessados em empresas que já possuam produtos ou *know-how* em tecnologias como PKI. Cada vez mais a segurança se transforma numa tecnologia embarcada, sendo que não faz mais sentido para uma multinacional investir no mercado de segurança brasileiro ou de qualquer outro país.

O Presidente da Beta também falou a respeito das principais barreiras às pequenas e médias empresas de Tecnologia da Informação no Brasil. O maior problema citado foi a excessiva carga tributária que as empresas precisam pagar, e que não está relacionada diretamente ao lucro. Como ele colocou a seguir:

> Se você monta uma empresa e consegue ter um faturamento, tudo bem. Mas caso ocorra uma crise, e o faturamento cair a zero, naquele mês em que você não faturou nada, ainda assim terá de arcar com impostos não relacionados diretamente ao lucro, mas sim a recursos humanos, a serviços, etc. Ou seja, é uma conta muito amarga de se ter. É preciso sempre dispor de recursos financeiros guardados, prevendo ter dois ou três meses sem faturamento algum, para garantir a sobrevivência da firma.

Essa barreira acaba prejudicando a criação de novas tecnologias no país, segundo o Presidente da Beta, pois a empresa acaba não podendo investir na pesquisa e no desenvolvimento de novos produtos, já que precisa realizar sempre projetos pontuais para sobreviver no mercado.

O Diretor de Tecnologia da Beta também citou a grande dificuldade em se vender projetos para o governo, afirmando que este exige das pequenas e médias empresas coisas que apenas as grandes companhias conseguem ter no Brasil. Porém as empresas pequenas e médias precisam vender para conseguir crescer e satisfazer aos critérios do governo, criando assim um círculo vicioso no mercado de tecnologia nacional, como ele colocou a seguir:

> É muito complexo vender produtos e serviços para o governo, pois são necessárias muitas viagens a Brasília e muito esforço para atender aos critérios dos editais. Apesar de que é satisfatório, já que a compra envolve sempre grandes cifras. O governo de qualquer país é responsável por movimentar a máquina. A recessão que a gente vive no Brasil é culpa do governo, que parou de comprar, e está arruinando diversas empresas em cascata.

A Beta chegou a perder uma venda para o BNDES, pois não estava com os impostos devidos em dia. Segundo o Diretor de Tecnologia, eles não estavam em dia justamente por não estarem vendendo há um bom tempo.

Outra barreira apontada foi a grande dificuldade em se estabelecer parcerias estratégicas no mercado de tecnologia brasileiro. Segundo o Diretor de Tecnologia, a maioria das empresas nacionais é oportunista, assim como eles próprios também muitas vezes o são, fruto da própria necessidade de sobrevivência que faz com que os empresários busquem o básico.

A Beta não possui nenhuma ligação com instituições de ensino superior, e considera isso um ponto fraco, como coloca o Presidente:

> Não temos essa conexão, e eu acho isso uma falha, acho que deveríamos ter. O dia-a-dia faz com que a gente não tenha tempo para isso. E esse tipo de coisa é difícil de acontecer via planejamento, geralmente acontece via pessoal, quando alguém vem com um trabalho de uma universidade. Talvez na universidade existam determinadas competências que sejam do nosso interesse, e assim poderíamos fazer um tipo de parceria.

6.2.3 Estratégia e gestão

A Beta é uma empresa bastante enxuta e que possui um modelo organizacional hierárquico, com um conselho de administração formado por três pessoas, eleitas anualmente pelos acionistas. Este conselho de administração é responsável pela definição das diretrizes da empresa, e por eleger o Presidente. Em março de 2003, a empresa passou por uma grande reestruturação organizacional, com a saída de dois de seus fundadores. Ao longo da história da companhia, sempre houve uma alta rotatividade de funcionários, principalmente pessoas da área comercial: "Nós chegamos a tirar um Diretor Comercial da filial de São Paulo com apenas quatro meses de trabalho". Apesar do modelo hierárquico, o Presidente coloca que, por se tratar de uma empresa muito pequena, existe um relacionamento muito aberto entre os diversos níveis da hierarquia. Mas ressalta que não se trata de uma estrutura matricial. Nas suas palavras: "é uma hierarquia muito flexível".

De forma diferente da Alfa, os investidores externos não parecem exercer uma interferência muito significativa, e a empresa acaba sendo comandada a partir das decisões dos poucos sócios fundadores. A busca por novos investidores também está centrada em manter a autonomia das decisões.

As estratégias empresariais na Beta são práticas, na visão do Presidente da empresa. Segundo ele, não há a aplicação de "conceitos acadêmicos". A empresa conta com fortes competências na área de pesquisa e desenvolvimento. O departamento de recursos humanos é terceirizado, mas segundo o Presidente da empresa, a estratégia de RH está na cabeça dos sócios, como ele colocou a seguir:

> A visão do grupo, do time, como captar as pessoas certas, está tudo na cabeça da gente. E como nosso forte está na nossa capacidade de P&D, damos preferência pelas pessoas vindas das melhores universidades do país.

A Beta possui apenas uma pessoa responsável por *marketing*. Questionado a respeito do pouco investimento nesta área, o Presidente da Beta disse que não há orçamento para isso na empresa. O que existe é a elaboração de *folders*, a realização de eventos para setores específicos da economia e uma acessoria de imprensa forte. Mas não há a realização de propaganda, até mesmo porque o tipo de produto da empresa é bem específico.

A área comercial da empresa é a que sente mais a falta de uma definição estratégica de competências, e onde a empresa possui as maiores dificuldades. Esta área, segundo o Presidente da Beta, requer visão estratégica, de *marketing*, capacidade de administrar contas de clientes, e fortes conhecimentos em tecnologia, resultando em um profissional bastante difícil de ser encontrado e recrutado.

Para a área de desenvolvimento, a Beta conta com um nível bastante forte de capacitação técnica dos seus funcionários, que envolve conhecimento e experiência com tecnologias não muito comuns no mercado de TI.

Em relação ao aprendizado na empresa, a Beta não possui nada formal, apesar de os sócios declararem que valorizam a educação continuada dos seus funcionários. Alguns funcionários da empresa possuem horário flexível para adaptar o trabalho aos seus estudos acadêmicos.

No que diz respeito à inovação, o Presidente da Beta considera a empresa inovadora. Na sua visão, o conceito de inovação ainda está preso à criação, à utilização ou à implantação de novas tecnologias de forma diferente do convencional. Ele também afirma que, de acordo com sua experiência nas palestras que realiza e nas visitas aos clientes, o mercado vê a Beta como uma firma bastante inovadora e que faz algo bastante diferente das demais: "O mercado nos enxerga como um instituto de pesquisas. A gente só faz coisas novas. Além do mais, pesquisa e desenvolvimento são fatores altamente estratégicos para a gente no momento".

Os sócios da Beta deram um passo importante pouco tempo depois de já estarem atuando no mercado de segurança, que foi a elaboração de um plano de negócios. Segundo o Diretor de Tecnologia da empresa, isso foi essencial para a captação de investimentos. Ele lembra que a maior parte dos investidores não entende do negócio específico da companhia. Através do plano de negócios, é possível apresentar aos investidores um planejamento prático e viável sobre os resultados de um possível aporte de capital realizado. Como ele colocou a seguir:

> É preciso mostrar um planejamento bem definido para os investidores, mostrar uma pesquisa de mercado do seu segmento, mostrar aonde você vai vender, quanto que vai vender, porque que vai vender, quanto que vai gastar com RH, com equipamentos, com *software*, telefone, viagem, treinamento, etc. Além disso, mostrar uma equação matemática que diga que, ao longo de X anos, será obtido Y de retorno.

Segundo o Diretor de Tecnologia, eles participaram de eventos promovidos pelo PROSOFT e pelo BNDES, onde diversos executivos de empresas que já haviam feito um plano de negócios davam relatos de sucesso ou fracasso. Todos os sócios da Beta foram unânimes em decidir por desenvolver um plano de negócios para a empresa.

Perguntado a respeito da necessidade de um aporte de capital, o Presidente da Beta disse que o mesmo não apenas ajuda a empresa, mas é indispensável na atual economia, principalmente para se fazer o *marketing* de um produto completamente novo. Na sua opinião, este *marketing* é construído a partir do zero ou comprado pronto. Em ambos os casos, é preciso muito dinheiro. Foi o que ocorreu com alguns *softwares* da empresa, que não existiam e não haviam sido contratados por nenhum cliente. A empresa teve que arcar com as despesas e o risco do desenvolvimento destes produtos, para o seu lançamento somente vários meses depois.

Para se adaptarem às mudanças ocorridas no cenário de competição global, os executivos da Beta foram obrigados a fazer alguns ajustes. Segundo o Presidente da empresa, os anos de 2001 e 2002 foram bastante complicados para o mercado brasileiro de TI, por causa da crise financeira do país, da desvalorização da moeda, da crise na Argentina, de crises políticas no governo, da crise energética e, em nível internacional, dos atentados de 11 de setembro. Além disso, toda a tensão gerada em torno das eleições de 2002 contribuiu em muito para a estagnação da economia. Com a desvalorização do real perante o dólar, as empresas que atuavam com *commodities* de segurança sofreram um forte impacto, e isso era exatamente o que garantia as maiores

margens da Beta. "Vendia-se muito *firewall* para as empresas de Internet", diz o entrevistado.

Uma das estratégias para vencer a atual crise é a busca por um novo aporte de capital, como já foi dito. A Beta está à procura de novos investidores, e com o dinheiro do investimento, os sócios dizem que o foco será a P&D aliada ao *marketing* de produto e comunicação. O Presidente da Beta cita que uma das maiores dificuldades atuais da empresa, em termos de estratégia, está relacionada com a venda do seu conhecimento específico. Apesar dos profissionais de excelente capacidade e dos produtos com altíssimo valor tecnológico e de conhecimento existentes na empresa, os seus diretores sentem grande dificuldade em fazer com que os clientes saibam o que está sendo oferecido e o potencial dos seus recursos humanos. Como ele coloca a seguir:

> Essa é a nossa grande dificuldade. É muito mais fácil você vender um produto como um computador, pois as pessoas possuem claramente a necessidade ou não possuem. Agora vender um conhecimento como o nosso, é extremamente difícil.

Além desse reforço na área comercial, um outro objetivo do novo aporte de capital, também de acordo com o Presidente da empresa, é o de acelerar a colocação de produtos no mercado antes da concorrência estrangeira:

> Esse é o nosso discurso: encurtar o "*time to marketing*". Queremos aumentar a equipe, comprar mais ferramentas e poder sobreviver sem a realização de projetos, tudo para conseguir colocar o mais rápido possível no mercado um novo produto de segurança. Isso é impossível de se conseguir sem investimento externo, tendo as contas da empresa muito fechadas. É preciso que alguém banque esse projeto.

Outra estratégia para vencer a crise, e que vem sendo utilizada pelos executivos da Beta, é a realização de parcerias e desvio da concorrência. De acordo com o Diretor de Tecnologia, todas as empresas de segurança existentes no Brasil poderiam ser parceiras da Beta. A empresa está dando bastante ênfase a essa estratégia, através da divulgação de notas na imprensa para informar a nova postura de atuação. O objetivo é fazer com que as empresas nacionais, que enxergam a Beta como concorrente, passem a vê-la como um possível parceiro estratégico. Como colocou o entrevistado:

> Muitas empresas de segurança deixam de fechar negócios por não possuírem determinadas competências. Quando você se abre para as parcerias estratégicas, você consegue realizar muito mais negócios e em todo o país, através de uma rede de parceiros. Você nunca deixa o seu cliente

> desatendido. Mesmo se você indicar um parceiro para determinado serviço, para o seu cliente continua sendo a sua empresa a porta de entrada.

A Beta não faz parte de nenhum grupo empresarial articulado. A estratégia acima vem suprir a necessidade por parcerias no mercado, pouco desenvolvida na empresa.

Veremos a seguir a atuação da Beta no mercado de segurança.

6.2.4 Atuação no mercado de segurança

A Beta começou a sua atuação no mercado sem a menor definição de foco estratégico. A empresa chegou a ter mais de 100 clientes quando atuava na área de segurança de redes (*Network Security*) e revenda de produtos. Segundo o Diretor de Tecnologia da empresa, existia uma quantidade muito grande de empresas "ponto com", o que representava um mercado muito forte para segurança de redes. Tudo isso veio abaixo com a crise da NASDAQ, e a Beta quase foi à falência. Só não o foi devido a uma mudança de foco abrupta para o mercado financeiro, tirando proveito do então recém lançado Sistema de Pagamentos Brasileiro (SPB). Com a crise, as empresas em geral cortaram os seus custos destinados à Segurança da Informação, com exceção das empresas financeiras.

A atuação da Beta nos dois últimos anos tem se concentrado cada vez mais no desenvolvimento de soluções em *software,* principalmente produtos. De acordo com a classificação da Sociedade SOFTEX (2002), a Beta possui um modelo de negócios do tipo produto/pacote, já que a maioria dos *softwares* desenvolvidos na empresa surgiram independentemente de clientes específicos, tendo como objetivo ganhar um mercado escalável. Apesar disso, a empresa já desenvolveu componentes de *software* específicos para alguns de seus clientes.

Em relação a Serviços Profissionais de Segurança, o Diretor de Tecnologia da Beta vê uma redução cada vez maior para esse mercado no Brasil. Segundo ele, houve um período em que implantar Políticas de Segurança era praticamente obrigatório para as empresas. Entretanto, os clientes tiraram pouco proveito desse tipo de serviço, que é muito caro e não possui resultados práticos imediatos, como foi colocado a seguir:

> Custa muito caro, e o gerente de TI do cliente fica com um monte de papel em cima da mesa, contendo os problemas de segurança e o que precisa ser feito para resolvê-los. Isso é o retorno que a maioria dos clientes que a gente visita nos dá. Os clientes hoje estão com menos orçamento e querem resolver

> seus problemas de maneira prática. Considero isso como uma evolução do mercado de segurança.

O que está mais perto de um serviço, realizado pela Beta, é a customização e o desenvolvimento de componentes de segurança específicos para o cliente. Neste caso, a empresa vende no final do processo um serviço, que inclui instalação, manutenção e atualização. Outro tipo de atuação mais voltada para serviços, da Beta, é o desenvolvimento de uma arquitetura de solução de segurança, que envolve dizer ao cliente o que ele deve fazer, como ele deve fazer e o quanto irá custar, mas sempre com foco no desenvolvimento de *software*.

Mas os sócios da Beta fizeram questão de deixar bem claro que a sua empresa não é uma consultoria. A idéia que eles possuem de uma empresa de consultoria está relacionada com a alocação de consultores no ambiente do cliente, em um período de tempo determinado, para a execução de um projeto.

A razão para tal, segundo o Diretor de Tecnologia da empresa, é que a atuação na área de consultoria possui uma "barreira de entrada" muito baixa, já que existe uma quantidade muito grande de empresas atuando (ou pelo menos dizendo que atua) na área de Serviços Profissionais de Segurança. A estratégia da Beta é se especializar cada vez mais em tecnologias com uma barreira de entrada alta. Isso pode ser visto pelo leque de tecnologias com o qual a empresa trabalha, como, por exemplo, *smart cards*, HSM, criptografia e certificação digital e desenvolvimento de *softwares* de segurança. Como foi colocado na entrevista:

> As competências técnicas para essas atividades não são facilmente encontradas no mercado. Não é qualquer programador ou qualquer técnico de segurança que está apto a atuar nessa área. É preciso recursos humanos com essas habilidades e com experiência na área, e é exatamente o que nós temos.

A Beta foi a única empresa pesquisada a possuir um foco específico na área de segurança. Segundo o Presidente da empresa, eles possuem um grande conhecimento na área de aplicação prática de criptografia e certificação digital. Apesar disso, a Beta vem sofrendo grande dificuldade em vender esse seu conhecimento, já que se trata de uma área ainda muito pouco divulgada, principalmente no Brasil. Como foi dito no item anterior, não existe ainda uma grande demanda para criptografia e certificação digital no país, por mais que se reconheça o fato de que estas tecnologias são de grande importância e potencial.

Dessa forma, um dos maiores obstáculos na atuação da Beta, atualmente, é como transformar o conhecimento de criptografia e certificação digital em produtos que sejam

de interesse do cliente. Devido a isso, a empresa está investindo bastante na área comercial, como já foi dito, com o intuito de criar soluções específicas para clientes específicos, baseadas nos produtos já existentes na empresa.

O produto de maior sucesso em vendas da Beta é um *software* voltado para criptografia e certificação digital, para uso em transações eletrônicas do Sistema de Pagamentos Brasileiro (SPB). Com a legislação implantada pelo Banco Central, o mercado para este tipo de *software* sofreu um grande salto, a partir de 2002. Vários grandes bancos do país são clientes da Beta, e mantém ainda contratos de suporte ao *software*.

O perfil do cliente da Beta é bem definido. Trata-se de um cliente que conhece Segurança da Informação e sabe muito bem o que a empresa faz e oferece. De acordo com o Presidente da companhia, não há condições de se buscar clientes de maneira genérica, principalmente em um mercado recessivo e em uma área específica da segurança:

> Nós não fazemos propaganda dos produtos aguardando que algum cliente se interesse, isso não existe para o nosso caso. Os clientes que nos procuram sabem muito bem o que querem e chegam até nós graças à nossa boa referência no assunto. Na atual recessão, não temos mais fôlego para ficar fazendo palestras e apresentações em todos os clientes possíveis.

É importante observar neste ponto que, apesar da Beta ser uma empresa com um modelo de produto/pacote, existe pouco investimento em *marketing*, quando deveria ocorrer justamente o contrário.

Os principais clientes da Beta estão no mercado financeiro. Os sócios da empresa vêm este mercado e o Governo como os mais importantes atores na área de Segurança da Informação, já que as empresas em geral estão muito pouco interessadas em segurança. A ICP Brasil e as legislações do SPB foram citadas como pontos positivos da ação governamental brasileira para fomentar o mercado de segurança, mas que ainda é preciso fazer mais. A Beta possui um produto que foi desenvolvido em cima de tecnologias de carimbo de tempo (*time stamp*), para a certificação digital de unidades de tempo. Entretanto, até hoje o governo não criou a legislação para tornar este tipo de tecnologia uma realidade no país, de forma que o produto da Beta está pronto, mas sem demanda no mercado brasileiro.

Para o mercado financeiro, segundo o Diretor de Tecnologia da Beta, é possível observar uma concentração ainda maior na capital paulistana, fazendo com que o mercado carioca fique cada vez mais reduzido para segurança.

Em relação ao mercado de Comércio Eletrônico, o Diretor de Tecnologia da Beta acredita que vá sempre existir alguma demanda, mas que nenhuma empresa de segurança pode tomar este segmento como foco de atuação. Como ele colocou a seguir: "Como as empresas de Comércio Eletrônico não estão tendo grandes margens de lucro no Brasil, elas estão cortando os investimentos em segurança, assim como as pessoas cortam o seguro do carro quando passam por crises financeiras".

O entrevistado afirma que cada vez mais o mercado passa a ver a empresa como uma desenvolvedora de produtos e soluções de segurança, com poucos ou quase nenhum concorrente no mercado nacional. Como já foi dito, a Beta abandonou a sua atuação no mercado de revenda, e se coloca como uma empresa desenvolvedora de *software* proprietário ou sob encomenda. Essa forma de se apresentar ao mercado também procura trazer um número maior de parceiros tecnológicos, os quais não vêem mais a empresa como uma concorrente. Ao "fugir" da atuação genérica na área de segurança, a Beta também está fugindo da concorrência, e se colocando como possível parceira de várias empresas.

Em relação ao futuro do mercado e à migração para os provedores de serviços e IDCs, o Presidente da Beta chegou a estudar a possibilidade de se tornar um Provedor de Serviços de Segurança (MSSP, como descrito no capítulo 5), com auxílio de uma consultoria estratégica do grupo Gartner, porém foram desaconselhados. Seria melhor deixar estes serviços para os *Data Centers* já existentes no país, e procurar estabelecer parcerias com os mesmos. Apesar disso, tais parcerias ainda não se concretizaram. O entrevistado também acha que o desinteresse das empresas brasileiras pelas questões de segurança tem colaborado para o pouco sucesso dos MSSPs no Brasil.

Ainda na visão do Presidente da Beta, a área de Segurança da Informação vai deixar de ser um mercado em si e vai estar embarcada nas outras Tecnologias da Informação. É o que também pensa o Diretor de Tecnologia da empresa, que citou o que ele chama de "comoditização" da Segurança da Informação:

> Acho que a segurança vai estar embarcada em outras tecnologias, e as grandes empresas de integração, os *full service providers*, é que vão cuidar disso. As empresas de segurança, tal como as conhecemos hoje, vão desaparecer.

Os sócios da Beta inclusive apontam para o fato de que grandes empresas, tais como IBM e HP, já possuem suas áreas de atuação em segurança, e que em breve se tornarão provedores de serviços completos. Isto reforça a estratégia adotada pela Beta de se firmar como uma empresa desenvolvedora de produtos de segurança, e não como uma empresa de segurança. De uma certa forma, os sócios querem ser reconhecidos no mercado como desenvolvedores de *software*, que no momento estão focados na área de segurança.

Os sócios também consideram que os IDCs vão se tornar, com o tempo, provedores de serviços gigantes, ou vão se associar/fundir com grandes empresas da área de tecnologia. Mas para o Brasil isso ainda levaria um tempo, de maneira que as empresas de Segurança da Informação ainda têm mercado no país. O Diretor de Tecnologia ressalta a importância de se realizar parcerias com grandes IDCs:

> Em nossa busca por novos aportes de capital, os investidores estão sempre nos perguntando se temos a intenção de fazer parcerias com IDCs. Vejo que isso é do interesse deles. Com o tempo, as empresas de segurança serão apenas uma parte de um IDC, e este, uma parte de um *full service provider*, como a IBM, por exemplo. Os investidores que conversam com a gente não visualizam mais um "mercado de segurança", eles estão interessados agora em empresas que possuam produtos de segurança.

A figura a seguir apresenta a evolução histórica da Beta, com base nas estratégias de atuação no mercado de Segurança da Informação apresentadas no item 5.3:

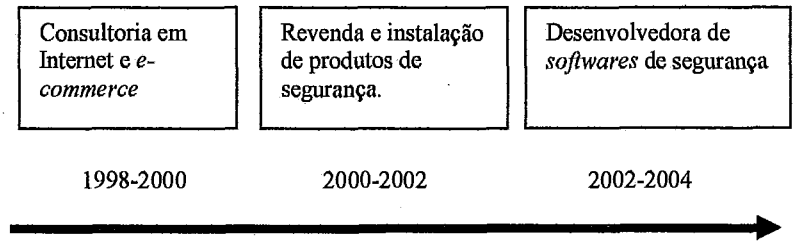


Figura 2 – Histórico de atuação da empresa Beta
Fonte: elaboração própria.

6.3 Empresa Gama

Para este estudo de caso, foram entrevistados o Diretor de *Marketing* e o Diretor de Desenvolvimento de *Software* da empresa Gama.

6.3.1 Histórico e evolução

A empresa Gama foi formada no final de 2001 por quatro sócios, a partir da saída de alguns profissionais da Alfa, como colocou um dos entrevistados:

> Éramos um grupo de pessoas que já trabalhavam há bastante tempo com Segurança da Informação. Em certo momento, pensamos que seria interessante abrir o próprio negócio, mas da nossa forma. E isso se deu no final de 2001, quando juntamos algumas pessoas e estruturamos o que viria a ser a nossa empresa.

A estratégia da Gama, que não sofreu grandes mudanças até hoje, é a de oferecer um portifólio de soluções o mais completo possível, tendo como foco a Segurança da Informação. Devido à experiência passada dos sócios, a Gama queria atuar no mercado de segurança de uma maneira bastante abrangente, sem estar ligada a determinados fabricantes para revenda de produtos, a uma tecnologia ou à realização de um tipo de serviço. Com este planejamento definido, a Gama começou a atuar de fato em janeiro de 2002.

Uma outra definição importante da Gama foi a sua visão de mercado. Desde o começo, a empresa concentrou a sua atuação na cidade do Rio de Janeiro. Segundo o Diretor de *Marketing*, isso se deveu, e ainda se deve, ao fato do porte da empresa, já que seria bastante difícil o deslocamento da equipe para outras praças. As outras cidades brasileiras, dessa forma, seriam atendidas através de parcerias, caso existisse alguma oportunidade. Como foi colocado a seguir pelo entrevistado:

> Hoje nós até temos projetos fora do Rio de Janeiro, mas através de venda casada com outras empresas, como ocorreu com um cliente no Nordeste. Não temos pessoal nosso disponível em outras cidades do Brasil. Por enquanto, nosso foco ainda é o Rio de Janeiro.

Durante todo o primeiro ano de funcionamento da Gama (2002), a empresa manteve sempre um quadro bastante enxuto de funcionários. No início, apenas alguns sócios dedicavam-se integralmente ao empreendimento, enquanto outros ainda estavam empregados em suas antigas companhias. Segundo o Diretor de *Marketing*, o primeiro marco de grande importância na história da empresa, que ocorreu também no ano de 2002, foi quando se criaram as condições necessárias para que todos os seis sócios pudessem vir trabalhar em tempo integral na Gama:

> Outros sócios que ainda não trabalhavam aqui saíram de onde estavam e vieram trabalhar aqui. Isso sim alavancou a empresa. Nós antes estávamos trabalhando e criando a base para que essas pessoas pudessem vir para cá.

Esse momento também marcou a principal mudança organizacional na história da Gama, já que a empresa precisou ser reestruturada. Foram alocadas pessoas para cada área específica: *marketing*; comercial; pré-venda técnica; desenvolvimento de *software*; tecnologia; administração e financeiro. Cada sócio ficou responsável por uma destas áreas e possuía suas respectivas equipes.

No final de 2002, os sócios da Gama precisaram se mudar para uma sala maior, devido à entrada de novos funcionários. Eles consideram isto como mais um marco, mas observam que tudo é feito sempre com bastante cautela e consciência: "não é questão ainda de alugarmos um andar inteiro. Estamos sempre com o pé no chão".

Atualmente, a Gama possui nove pessoas trabalhando fixamente na empresa, e apesar de não revelarem o faturamento anual, os seus sócios a classificaram como uma empresa de porte micro.

6.3.2 A empresa no mercado de TI

A Gama é uma empresa ainda muito nova, mas que começa aos poucos a se consolidar no mercado brasileiro de TI. Os seus sócios acumularam uma larga experiência no mercado de segurança, devido às suas passagens por empresas anteriores. Esta experiência criou uma cultura forte entre eles, já que, assim como os fundadores da Alfa, os sócios da Gama, em sua maioria, são originários do curso de Informática da UFRJ. Segundo o Diretor de Desenvolvimento de *Software*, essa vivência no meio acadêmico, e posteriormente no empresarial, foi de extrema importância para a criação da empresa e o desenvolvimento das competências necessárias, principalmente na área de *software*.

A impressão que os executivos da Gama têm do mercado brasileiro de TI é de uma árdua competição, onde as empresas brasileiras, principalmente as pequenas e médias, estão sempre em desvantagem. Segundo o Diretor de *Marketing* da Gama, as empresas brasileiras que obtiveram sucesso no mercado de TI são "exceções à regra". Uma das maiores dificuldades citadas por ele foram as limitações dos empresários brasileiros:

> O mercado brasileiro não é forte em tecnologia. Existem casos de sucesso de empresas que desenvolvem ERP, uma ou outra que desenvolve bons produtos de tecnologia, etc. E sinceramente eu não vejo muito como o mercado mudar, em um curto espaço de tempo, principalmente pela falta de maturidade e capacitação do empreendedor brasileiro.

O sócio também citou como um grande problema a visão de curto prazo do empresário brasileiro, que procura sempre enriquecer muito rapidamente: "O empresário quer investir hoje pra ter retorno em no máximo dois anos. Se for para criar uma empresa hoje, com expectativa de retorno em 20 anos, não serve".

As competências relacionadas ao desenvolvimento de *software* são bastante desenvolvidas na Gama, fruto também da experiência passada dos sócios em gerir o departamento de desenvolvimento de *software* da empresa Alfa. Na Gama, existe o desenvolvimento de *software* de alto valor agregado, mas também são realizados pequenos projetos, com tecnologias mais simples. Apesar da empresa possuir produtos, estes sempre derivaram de projetos de *software* contratados por clientes específicos.

A companhia nunca participou de programas para o fomento à exportação de *software*, entretanto isto não está fora dos planos. Segundo o Diretor de Desenvolvimento de *Software*, os produtos da empresa já são projetados de maneira a suportar vários idiomas: "Nossos dois principais produtos de *software* foram desenvolvidos com suporte multilingüe. Nós temos consciência de que *software*, restrito apenas ao mercado nacional, é impossível".

Este sócio também relatou que está ciente da necessidade da certificação CMM para a exportação de *software*, mas que a empresa ainda está em fase de desenvolvimento dos seus processos. Além disso, faltam os recursos financeiros para realizar a certificação.

Uma outra estratégia para a exportação, que vem sendo utilizada pela Gama, é a utilização de canal com empresas estrangeiras. Um dos clientes da Gama adotou um de seus principais produtos, um sistema de monitoramento de *sites*. Este cliente é uma empresa multinacional que já cogitou a idéia de implantar o produto em todas as suas unidades da América Latina. Como colocou o Diretor de *Marketing*:

> Não se trata de uma estratégia voltada diretamente para a exportação, mas estamos aproveitando a oportunidade de possivelmente aparecer no mercado exterior. Somos uma empresa que gosta de dar um passo de cada vez, e ainda há muito mercado no próprio Rio de Janeiro. Por isso não estamos nos direcionando totalmente para essa coisa de exportação.

Em relação a investimentos e aportes de capital, desde o início de 2002 os sócios da Gama decidiram não procurar recursos financeiros externos. Optaram por investir dinheiro próprio, seja do faturamento da companhia ou dos próprios sócios. A principal justificativa que foi dada para essa estratégia, e que se baseia na experiência passada dos

sócios da Gama trabalhando na empresa Alfa, é que um investidor externo interfere muito nos rumos da empresa, e acaba trazendo mais problemas do que benefícios. Eles chegaram inclusive a serem procurados por investidores do Rio de Janeiro e até de São Paulo, que de alguma forma tomaram conhecimento da empresa e do nome que ela já começava a fazer no mercado.

O Diretor de *Marketing* da Gama até concordou que um aporte de capital é necessário para grandes saltos no mercado e para a exportação de *software*:

> Se você pensar em termos de um salto muito grande, realmente é necessário. Dependendo da visão adotada pela empresa, se ela for muito grande, ao invés de um passo de cada vez, provavelmente você não vai sair do lugar sem um aporte de capital.

Este sócio também citou uma série de barreiras que, na sua visão, freia o desenvolvimento das empresas de pequeno e médio porte no Brasil. Um dos exemplos citados foi a dificuldade que existe em se conseguir vender projetos para o governo:

> Esse é um problema que sempre existiu, a começar pelos editais de contratação. Quase sempre requer um faturamento mínimo, um tamanho mínimo para a empresa como um todo, a existência de certificações de qualidade, abrangência nacional, etc. Nós só atuamos no Rio de Janeiro, somos pequenos e não temos recursos para atender a todas essas exigências.

As próprias empresas privadas também colocam uma série de dificuldades para comprar de empresas pequenas como a Gama. Em uma das entrevistas, foi relatado que a Gama já perdeu vários projetos por essa razão:

> Vários clientes já nos disseram francamente: achamos excelente o seu produto, mas se vocês entrarem numa concorrência aqui dentro, sua empresa será analisada, e a primeira coisa que vão perguntar é o tempo que vocês estão no mercado. E isso vai tirar vocês imediatamente da disputa.

Uma outra barreira mencionada foi a falta de reconhecimento do *software* e da tecnologia nacional no exterior. Segundo o Diretor de *Marketing*, a visão que se tem fora do Brasil é a de que nós não sabemos fazer tecnologia:

> Se nós fossemos vender para todo o mercado brasileiro, isso representaria apenas uma pequena parcela do mercado mundial, mas já exigiria um grande esforço da empresa. E para vender no exterior (nos EUA, por exemplo, que representa hoje 40% do mercado mundial de *software*), existe uma série de barreiras. Você precisa de dinheiro para colocar o produto no mercado externo, precisa participar de algum projeto de fomento do governo, precisa ter CMM, etc.

O peso da carga tributária no Brasil, para as pequenas e médias empresas, foi bastante criticado pelos sócios da Gama. Também foram citados os juros bastante altos pagos em empréstimos e os custos de abertura, manutenção e fechamento de empresas. Segundo os sócios, o governo não possui uma política que tenha como alvo essas questões para as pequenas e médias empresas no Brasil.

Também foram relatadas grandes dificuldades em relação à cooperatividade das empresas brasileiras de TI. Um dos entrevistados disse que gostaria de estar bem mais articulado no mercado de segurança, mas as outras empresas estariam sempre colocando barreiras:

> A gente gostaria muito de estar cooperando com outras empresas. Por exemplo, a maioria das pessoas que trabalham aqui veio de outras empresas de segurança. Por que não trabalhar em conjunto com estas empresas? Vamos aproveitar o melhor de cada um. Eles possuem lá uma marca, uma força comercial, uma penetração grande no mercado, mas de uma hora para outra, perderam uma equipe. E a gente tem a equipe. Por menor que seja, temos a equipe, pessoal com conhecimento, pessoal especializado. Será que não daria para atuar em conjunto?

Os sócios da Gama atribuem esse problema à cultura nacional de desconfiança mútua, e das dificuldades geradas pela crise financeira, que fazem os empresários pensarem de forma muito imediata.

No que diz respeito à interação com o meio acadêmico, a Gama possui um convênio com a PUC do Rio de Janeiro, para o desenvolvimento de novas tecnologias. Entretanto, os entrevistados confessaram que este convênio tem sido muito pouco utilizado. Enfatizam inclusive que, apesar da maioria deles ser proveniente do curso de Informática da UFRJ, não existe nenhuma ligação da empresa com esta universidade.

A respeito da maneira como o governo poderia ajudar no fomento da indústria nacional de TI, os executivos da Gama consideram que o Estado até tem feito coisas consideráveis na área de segurança, ao investir bastante nos serviços de Governo Eletrônico que vêm sendo disponibilizados. Mas que isso é mais uma conseqüência, sem um planejamento específico para a área. Na visão do Diretor de Desenvolvimento de *Software*, deve-se investir mais em projetos parecidos com o Softex:

> Hoje nós estamos muito fracos nessa área. Se nos compararmos à Índia, por exemplo, temos muito menos empresas e pesquisadores. O governo também deveria ajudar com investimento a fundo perdido. Hoje, para uma empresa conseguir algum empréstimo no banco, é preciso pagar taxas absurdas. Então

> eu acho que o governo é o grande alavancador, ele é o maior comprador do mercado, mas infelizmente não está exercendo este papel.

Outro ponto em que o Estado está deixando a desejar, na visão dos diretores da Gama, diz respeito à formação dos profissionais no Brasil. Foi dito que o ensino universitário no Brasil, para a área de ciências da computação, é bastante fraco e com currículos desatualizados em relação ao resto do mundo e às demandas de mercado. Além disso, não existe quase nenhum enfoque na área de Segurança da Informação nos cursos de Informática brasileiros, e poucos alunos que se formam acabam indo trabalhar com desenvolvimento de *software*. Na visão dos sócios, precisamos criar mais "doutores no assunto", para podermos competir com países como a Índia.

6.3.3 Estratégia e gestão

Na Gama não existe um processo de gestão definido, sendo que os sócios administram a empresa de maneira informal. A organização é bastante simples, onde cada sócio é responsável por uma área específica e pela sua equipe. Como já vimos, a empresa conta com seis sócios e três colaboradores que trabalham como prestadores de serviço.

Os diretores da Gama já chegaram a elaborar uma espécie de rascunho de um plano de negócios para a empresa, segundo eles, para uma futura procura por investimento externo. Mas como preferem no momento contar com o próprio investimento, ainda não foi dado um foco no planejamento estratégico. Como colocou o Diretor de Desenvolvimento de *Software*:

> Temos um rascunho de um plano de negócios. Pensamos em elaborar um para a eventualidade de atrair algum investimento, mas tudo que fizemos até agora foi usando nossos próprios recursos e esforço pessoal de cada um. Não fizemos um BP (*business plan*) formal durante o processo de criação da empresa, ficou na informalidade mesmo.

Não há também uma pessoa exclusivamente responsável por estratégias, ou por analisar o mercado e prever as suas direções. Apesar disso, os executivos da empresa costumam acompanhar os meios de comunicação e agir da melhor maneira possível. O Diretor de *Marketing* disse não possuir nenhuma formação sofisticada em gestão e estratégia empresarial, entretanto eles estão sempre procurando utilizar as melhores práticas do mercado, de acordo com as possibilidades da empresa: "Temos em mente o que é preciso fazer, mas nem sempre conseguimos. Estamos sempre procurando

direcionar a empresa para aquilo que existe de melhor em termos de organização, métodos, processos, práticas, etc".

Segundo o Diretor de Desenvolvimento de *Software* da Gama, eles estão em vias de formalizar os seus processos internos de qualidade, mas ainda não existe nada definido. A conscientização da importância destes processos foi trazida como uma certa "herança" do tempo em que os sócios da Gama trabalharam na empresa Alfa.

Como já foi dito, os produtos de *software* desenvolvidos na Gama utilizam os recursos financeiros do próprio cliente. Nenhum produto é desenvolvido na empresa sem uma demanda direta de algum cliente, como colocou o Diretor de *Marketing*:

> Nós não desenvolvemos um produto só por desenvolver, não temos uma grande idéia de noite e iniciamos um projeto no dia seguinte. Sempre desenvolvemos um produto para atender a uma necessidade específica de um cliente. Terminado este projeto, nós analisamos o potencial daquele produto, para então ver se o mesmo pode ser oferecido a outros clientes.

O que é desenvolvido é sempre uma solução para um cliente, e esta solução pode ou não virar um produto. Isso acaba dependendo do tamanho do mercado e da demanda de outros clientes. O tempo para se lançar um produto, neste caso, é função da demanda para o mesmo:

> Certamente, se tivéssemos um aporte de capital, ao invés de termos uma equipe de cinco pessoas desenvolvendo, teríamos algo em torno de quinze, diminuindo assim o tempo para lançar o produto no mercado. Mas optamos por uma estratégia diferente.

A Gama foi obrigada, mais recentemente, a realizar mudanças estratégicas para vencer as crises nacionais e mundiais da economia. A diminuição nas compras realizadas pelo governo, no ano de 2003, não afetou diretamente a Gama, já que a empresa não possui muitos clientes na área pública. Entretanto os sócios relatam como maior problema a queda das compras feitas pelas empresas em geral, na área de TI. A principal estratégia usada neste momento foi o reforço da área comercial, como colocou um dos entrevistados:

> Nós continuamos a ter apenas uma pessoa responsável pela área comercial da empresa, entretanto todos, no final das contas, fazem parte da equipe comercial. Qualquer simples telefonema, que pode ser responsabilidade de qualquer um aqui dentro, pode trazer negócios para a gente. Mesmo com um mercado recessivo, mesmo o número de clientes e o faturamento não sendo aqueles que a gente gostaria, todas as ações que temos feito têm sido no sentido de reforçar a nossa atuação comercial.

O Diretor de *Marketing* também disse que, apesar de todas as mudanças para vencer a crise, não foram economizados recursos em áreas de necessidade: "Aquilo que a gente achava necessário para estar prestando um bom serviço de qualidade, nós mantivemos com altas prioridades".

Quanto à inovação, os sócios consideram a Gama inovadora, mas principalmente devido às competências individuais dos recursos humanos. Segundo eles, o perfil dos sócios é bastante diferenciado, incluindo várias competências, na maioria dos casos obtidas da experiência anterior destes profissionais trabalhando na Alfa.

Mas o maior destaque dado pelo Diretor de Desenvolvimento de *Software*, em termos de inovação, está no campo da tecnologia, por estarem sempre buscando novas soluções para os clientes: "não estamos limitados aos serviços básicos que a maioria das empresas realiza". As competências técnicas dos sócios da Gama, na área de desenvolvimento de *software*, que foram desenvolvidas na época em que os mesmos trabalhavam na empresa Alfa, são um dos pontos fortes.

A Gama possui dois *softwares* desenvolvidos, um de monitoramento de *sites* e outro de consolidação de registros de *log* de segurança que, segundo o Diretor de *Marketing* da companhia, não possuem equivalentes no Brasil, apenas no exterior, e que se tornaram produtos de sucesso. Segundo ele, a empresa também trabalha atualmente em uma solução de segurança para telefonia baseada em IP, com o uso de certificação digital, que também será inédita:

> Estamos sempre buscando soluções novas para resolver os problemas dos clientes, seja um produto inovador ou um discurso novo para vender um serviço antigo. Procuramos criar soluções específicas do mesmo produto e serviço para clientes diferentes. Acho que nossos profissionais estão acima da média no que diz respeito à inovação.

P&D é um fator bastante importante na estratégia da empresa, de acordo com o Diretor de Desenvolvimento de *Software*, apesar da Gama não contar com recursos financeiros para investimentos nessa área. Segundo ele, como em geral são os próprios sócios a tocar projetos técnicos, eles possuem a consciência de que precisam se atualizar e pesquisar sempre coisas novas, mesmo não existindo nenhum processo formal para isso dentro da empresa.

Já o departamento de *marketing* é terceirizado, mas considerado de grande importância na estratégia da Gama. Eles possuem um diretor para as questões de *marketing*, e contrataram uma firma terceirizada que é responsável pelo *site*

institucional da Gama e pela apresentação da empresa ao mercado. Sempre que podem, os sócios estão escrevendo artigos para revistas.

Mesmo com as dificuldades já citadas no item anterior, a Gama vem tentando estabelecer uma estratégia de parcerias. O que seus diretores estão fazendo é procurar por parceiros que complementem os seus serviços, mas sem que haja um mínimo de concorrência. Um exemplo são as parcerias com empresas desenvolvedoras de *sites* ou aplicações para a *Web*, onde a Gama entraria com a parte de segurança. O grande problema, na formação de parcerias da Gama com outras empresas de segurança, está na sua proposta de atuação, que é bastante ampla, gerando concorrência em quase todas as tentativas de cooperação.

6.3.4 Atuação no mercado de segurança

Como já foi colocado, a Gama possui uma atuação bastante abrangente no mercado de segurança. Os seus sócios, durante as entrevistas, não classificaram a empresa como sendo voltada para produtos ou serviços, mas sim como uma empresa que oferece "soluções de segurança". Estas tais soluções, de acordo com os entrevistados, podem conter produtos ou serviços, dependendo do caso específico. A atuação da Gama pode ser subdividida em três áreas principais, a saber:

- Consultoria em Serviços Profissionais de Segurança, incluindo todos os serviços básicos de elaboração de Política de Segurança, Análise de Vulnerabilidade e testes de invasão. A empresa também realiza análise de aplicações, com foco em segurança no desenvolvimento de *software*.
- Revenda e integração de produtos, que engloba a comercialização, implantação e configuração de produtos e tecnologias de TI relacionados a segurança, tais como *firewalls*, roteadores, VPNs, antivírus e PKI.
- Desenvolvimento de *software*. Nessa linha de atuação, a Gama aproveita o conhecimento da maioria de seus sócios, os quais possuem um forte histórico na área de *software*, para desenvolver soluções específicas que atendam às necessidades dos clientes. O objetivo é fornecer a estes a camada de segurança de *software*, a que eles não possuem domínio, e pode variar desde o desenvolvimento de complexos sistemas de segurança em C++ a páginas *Web* escritas em ASP.

Eventualmente, a Gama também realiza treinamentos de segurança no desenvolvimento de *software*, para um público alvo de analistas de sistemas. Segundo o

Diretor de Desenvolvimento de *Software*, os cursos abordam o projeto e especificação de sistemas de segurança, além de práticas seguras a serem executadas por uma equipe de *software*, tais como a segurança do código fonte e o controle de acesso ao local de desenvolvimento.

Em relação aos clientes, os sócios da Gama também possuem uma visão bastante ampla de atuação. Um dos entrevistados justifica isso pelo fato de eles ainda estarem passando por um momento de estruturação:

> Nós não definimos qual o tamanho da empresa cliente que vamos dar foco, nem o segmento, se é governo, área financeira, indústria, etc. A Gama só tem dois anos, ainda estamos criando a nossa cultura. Quando fundamos a empresa, tínhamos uma quantidade de clientes com os quais nós mantínhamos contato. Estes clientes foram o nosso foco inicial, mas sem nenhum critério específico. Nós trabalhamos com qualquer tipo de projeto, grande ou pequeno.

O único segmento de clientes que está um pouco fora do escopo da Gama é o mercado financeiro, apesar dos sócios concordarem que é um dos mais importantes mercados para a área de segurança. Desde o início, os fundadores da Gama foram determinados em não atuar, por exemplo, em projetos do Sistema de Pagamentos Brasileiro (SPB), como foi relatado em uma das entrevistas: "Algumas pessoas achavam loucura isso da nossa parte, já que todas as empresas de segurança estavam ganhando dinheiro com o SPB".

Uma das razões para esse desvio do mercado financeiro, segundo o Diretor de *Marketing* da Gama, foi a concentração da empresa na cidade do Rio de Janeiro. As empresas financeiras e os bancos estão em sua grande maioria baseados em São Paulo. Além disso, a empresa estaria entrando um pouco atrasada nesse mercado, que já estava sendo atendido por empresas maiores. Portanto, procurou-se atuar no mercado restante, que estava então ficando desatendido, como foi colocado a seguir:

> Na nossa visão, a "mina de ouro" do SPB algum dia acabaria, fazendo com que todas as empresas de segurança se voltassem para os outros segmentos. Quando isso ocorresse, e isso está ocorrendo agora, essas empresas teriam que concorrer com a gente.

Para os sócios da Gama, atualmente existe uma grande quantidade de empresas atuando no Brasil e que estão focadas na venda e implantação de ferramentas de segurança. Essas empresas acabam se tornando parceiras de grandes fabricantes internacionais, tais como Check Point® na área de *firewall*, e conseguem dessa forma

bons descontos nos preços dos produtos. Entretanto, não existe quase nenhuma consultoria sendo feita por esse tipo de empresa, muito menos desenvolvimento de *software,* e a Gama coloca-se como uma alternativa, oferecendo um portifólio completo no mercado, como colocou o Diretor de *Marketing*:

> Não que seja melhor adotar essa ou aquela estratégia de abordagem do mercado. Essas empresas que apenas atuam como revenda ganham bastante dinheiro, têm suas vantagens. Mas o nosso foco é outro. Somos parceiros de vários fornecedores, sem contar com vantagens dadas por nenhum deles. Nossa idéia é oferecer ao cliente uma solução de segurança que resolva o seu problema, de acordo com os seus recursos financeiros.

O entrevistado ainda observou que atualmente todas as empresas de TI dizem oferecer serviços de segurança e entender do assunto, o que gera um grande problema devido à pouca idade do mercado:

> De uma hora pra outra, o mercado sofreu uma avalanche de empresas prestando segurança, e aquelas empresas que já prestavam algum serviço de redes, também passaram a fazer segurança. Ou seja, o mercado hoje está bem mais competitivo do que há dois anos atrás.

Devido ao escopo de atuação da Gama ser bastante grande, a empresa acaba tendo como concorrentes desde as pequenas empresas até os grandes provedores de segurança. O Diretor de Desenvolvimento de *Software* citou, por exemplo, que a empresa já perdeu vários negócios onde o concorrente entendia pouco ou nada de segurança, mas era uma companhia conhecida do cliente:

> Muitas dessas empresas, por exemplo, cuidam da rede do cliente. Quando ocorre um problema de segurança, uma vez que eles já estão lá dentro, eles acabam fazendo mais este serviço. Embora não façam o melhor serviço do mundo, o cliente já está acostumado com eles. Esse é um tipo de empresa com o qual a gente cada vez mais vem concorrendo no mercado.

Além dessas empresas, a Gama cita as outras conhecidas do mercado de segurança como suas concorrentes, como, por exemplo, as empresas Alfa e Beta. Outras empresas concorrentes são aquelas que trabalham com revenda e implantação de ferramentas, já citadas.

Em relação às grandes empresas do tipo IBM®, Arthur Andersen® e Deloite Touchet®, que atuam com Serviços Profissionais de Segurança, a Gama apenas concorreu uma única vez com a primeira. Segundo um dos sócios entrevistados, eles não concorrem muito com estas empresas, pois as mesmas costumam entrar em

negócios grandes do governo, fora da linha de atuação da Gama. Todavia, são vistos como concorrentes.

Sobre o futuro do mercado de segurança, a Gama não vê uma migração total para os *Data Centers* e MSSPs. Segundo o Diretor de *Marketing*, ao menos no Brasil, os IDCs ainda não obtiveram sucesso e a sua maior finalidade, a hospedagem de servidores, possui grande ociosidade na maioria dos casos. Além disso, ele acredita que haverá espaço para todos no mercado de segurança brasileiro, pelo menos por um bom tempo:

> Com certeza não serão todas as empresas a migrar para os IDCs. Já vimos casos de clientes falando que iriam migrar seus servidores para um IDC, por questões de segurança. E já vimos outros casos de clientes falando que não iriam realizar tal migração, também por questões de segurança. Ou seja, as empresas pensam diferente nesse ponto, possuem objetivos e recursos orçamentários completamente diferentes. Os preços cobrados pelos IDCs são muito caros, e nem todos os clientes podem arcar com isso.

O entrevistado conclui dizendo que, na sua visão, existem no mercado brasileiro preços, serviços e qualidades diferenciadas para todos. Para ele, o mercado de segurança vem amadurecendo cada vez mais com o tempo, e que ainda falta o estabelecimento e a difusão de uma série de novas tecnologias, como PKI, por exemplo, principalmente no Brasil. Tais tecnologias ainda precisam, dessa forma, ser mais bem trabalhadas e divulgadas para que se possa criar a demanda necessária: "o mercado de segurança ainda está muito atrasado no Brasil".

Por ser uma empresa nova, a Gama não apresenta um histórico evolutivo e seu foco estratégico não sofreu mudanças significativas. A figura a seguir apresenta a estratégia de atuação da empresa nos dois últimos anos, com base no item 5.3:

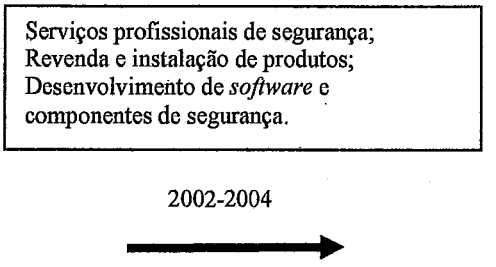


Figura 3 – Atuação da empresa Gama

Fonte: elaboração própria.

6.4 Análise dos resultados

Após a descrição dos estudos de casos nos itens anteriores, fazemos aqui uma síntese das informações obtidas e uma análise comparativa entre as empresas estudadas.

A primeira observação diz respeito à importância exercida pelo meio acadêmico na formação das empresas, e que foi citada no item 3.2 deste estudo. Mesmo a Beta, cujos fundadores não possuem esta cultura, está podendo desfrutar dos seus novos funcionários da área de *software*, muitos dos quais são amigos da época de faculdade e estudaram em universidades tais como UERJ e UFRJ. Mas o caso mais evidente de benefício está na Alfa e, por conseqüência, na Gama. Foi na UFRJ que os sócios da Alfa tiveram o primeiro contato com tecnologia de ponta, e inovaram ao perceber, ainda em 1985, o potencial da área de segurança para o mercado de Tecnologia da Informação.

Foi possível observar nos estudos de caso que as três empresas começaram a sua organização de maneira bastante informal, onde os sócios fundadores realizavam todas as tarefas, desde as mais administrativas até as técnicas. Isso acabou por criar uma cultura de flexibilidade dentro dessas empresas. Esta flexibilidade é um requisito essencial para a competitividade, apontado no item 4.1.1.2, e que procura inserir todos os funcionários da empresa na esfera das estratégias competitivas.

As empresas Alfa e Beta viveram em suas histórias uma mudança constante de foco estratégico, visando tanto o aproveitamento de novas oportunidades quanto a reação às crises, onde a flexibilidade foi um fator diferencial. A Alfa, por ter um processo de gestão que evoluiu com o tempo e se tornou bem definido, possui uma maior facilidade nas mudanças estratégicas e adaptações ao mercado, o que pode ser observado nos relatos dos entrevistados e vivência com funcionários da empresa.

A elaboração de um planejamento de negócios (*business plan*) trouxe vários benefícios para as empresas Alfa e Beta, sendo que a Gama ainda pretende realizar o seu planejamento formal. Isso também está de acordo com a necessidade de uma definição dos objetivos estratégicos da companhia, citada no capítulo 4. Apesar disso, apenas a Alfa pareceu estar usando este planejamento para efetivamente gerir a empresa, subdividindo os objetivos do plano em ações práticas dentro da companhia.

Os empresários entrevistados classificaram as empresas bem sucedidas na área de TI como exceções à regra, e que o empreendedorismo para a área de tecnologia no Brasil é bastante desmotivador, com todas as condições adversas. Um ponto em comum levantado por todos os empresários entrevistados foi a necessidade de uma legislação

trabalhista particular voltada para os profissionais de TI e da redução do Custo Brasil. As empresas Beta e Gama também se queixam de não conseguirem realizar vendas para clientes governamentais, devido às exigências consideradas um tanto "abusivas". Em geral, eles levantaram os mesmos problemas observados na pesquisa feita pela Sociedade SOFTEX (2002), como apresentado no item 3.4.2.2, e reforçam a necessidade por políticas que tenham como objetivo o desenvolvimento das PMEs e da sua capacidade competitiva, como foi discutido nos itens 4.2.3 e 4.3.1.

A opinião dos executivos da Alfa também divergiu dos demais empresários das duas outras empresas (Beta e Gama) no que diz respeito aos programas de fomento, como o Softex, por exemplo. Segundo os primeiros, estes programas deveriam ser constituídos principalmente de recursos privados, sem muita participação do governo, e deveriam possuir requisitos bastante rígidos para a participação das empresas. Já os sócios da Beta e da Gama se queixaram bastante destas exigências. Uma interpretação possível é que a Alfa, por ser a empresa com o processo de gestão mais sofisticado e que atende aos requisitos dos programas de fomento, defende um mercado mais fechado, excluindo empresas pequenas e do tipo *start-up*, beneficiando-se assim da sua posição já alcançada no cenário de TI brasileiro.

A definição de objetivos estratégicos e de escolha por um foco de atuação, tão necessária e apontada no capítulo 4, demorou a ser feita nas empresas. Uma característica em comum observada foi um certo deslumbre pelo mercado de Internet, principalmente para as empresas mais antigas, a Alfa e a Beta. Com o crescimento da bolha das empresas "ponto com", os executivos daquelas companhias não se contiveram em investir, de todas as formas possíveis, para entrar no mercado de Internet. Essa foi uma das causas das crises financeiras que abateram essas empresas nos anos seguintes, quase levando uma delas, a Beta, à falência.

A Gama foi a única das três empresas a adotar uma estratégia mais comedida em relação aos seus objetivos. Tanto a Alfa quanto a Beta, em determinados momentos, definiram a estratégia de dar um salto muito grande, investindo em determinado produto ou linha de atuação. A Alfa, por exemplo, obteve investimento de capital e mudou as suas instalações de um andar de um prédio no centro do Rio para um prédio inteiro, de quatro andares. A Beta também se mudou para uma sala muito maior quando recebeu o aporte de capital e investiu grandes somas de dinheiro em ferramentas de desenvolvimento e equipe. Nas entrevistas, os executivos das duas empresas afirmaram que sempre tiveram em mente expandir a atuação para o Brasil inteiro e para o mundo.

É importante frisar que tais "planos audaciosos" tornaram estas empresas viáveis apenas através de aportes externos de capital.

Os profissionais da área de *software* foram citados, nas entrevistas, como bem capacitados, e isso confirma o potencial dos recursos humanos da área de pesquisa e desenvolvimento no Brasil, descrito nos itens 3.2 e 3.4.2. Nas três empresas, ainda que em processo de elaboração na Gama, as metodologias de desenvolvimento de *software* foram criadas pelos próprios analistas.

Apesar disso, alguns entrevistados apontaram que os novos funcionários costumam possuir poucos conhecimentos relativos às questões mais voltadas para a visão de negócio e empreendedorismo, questões que segundo eles também deveriam ser estimuladas e desenvolvidas no ambiente acadêmico. Outra carência identificada nos cursos de Informática diz respeito à área de Segurança da Informação. Segundo todos os entrevistados, não se ensina praticamente nada sobre este tema nas universidades.

A partir dos estudos de caso, observamos que a certificação ISO mostrou-se ineficaz para a exportação de *software*. A Alfa, única empresa a conseguir alguma certificação de qualidade, não obteve vantagens ao tornar o seu departamento de *software* certificado como ISO 9001. A certificação foi utilizada no mercado brasileiro mais como um componente de *marketing*. Na opinião dos empresários entrevistados, o CMM parece ser o tipo de certificação a ser perseguido para a exportação de *software* nacional.

A Alfa também se sobressai em relação à gestão do conhecimento, um assunto considerado de grande importância para as empresas de TI, como apresentado nos itens 4.1.1 e 4.1.2. A empresa possui um processo de aprendizagem bem definido, com uma metodologia de execução de serviços e uma base de conhecimentos interna, estando assim mais independente de pessoas particulares. Na sua história, a Alfa sofreu grande rotatividade de funcionários, principalmente nos últimos tempos, quando o sistema de gestão do conhecimento já estava definido. Tanto a Beta quanto a Gama parecem depender bastante dos seus recursos humanos, podendo ter sérios problemas com a saída de alguns deles.

Os sócios das empresas pesquisadas também colocaram que o governo deveria encarar as tecnologias de segurança ainda pouco difundidas, tais como PKI e certificação digital (citadas no item 5.2.3), como um investimento a ser feito agora, nas empresas nacionais, para se colher os frutos no futuro. Segundo eles, essas tecnologias

serão difundidas largamente em um futuro próximo, e poderíamos estar desenvolvendo conhecimentos e produtos nesta área destinados à exportação.

Das empresas pesquisadas, nenhuma realizou registro de patentes industriais. Apesar disso, todas elas possuem o código fonte de seus produtos de *software* devidamente registrados quanto à propriedade intelectual.

O quadro a seguir resume as principais características encontradas nas empresas, de acordo com os modelos mais importantes vistos na revisão teórica:

	Alfa	Beta	Gama
Modelo de negócios (*software*)	-	Produto/pacote.	Serviços de baixo e alto valor.
Estratégia competitiva	*Marketing* voltado a clientes específicos.	Inovações radicais (*breakthrough*).	Desenvolvimento de soluções e sistemas específicos.
Articulação global	Inserção em cadeias produtivas globais (Tipo B)	Parceria em redes globais (Tipo A)	Atuação em mercados não globalizados (Tipo C)
Atuação no mercado de segurança	Soluções de segurança integral.	Desenvolvimento de produtos de segurança.	Revenda e instalação de produtos; serviços profissionais de segurança; desenvolvimento customizado de software.

Tabela 11 – Análise dos resultados dos Estudos de Casos

Fonte: elaboração própria.

Os itens de destaque acima são o modelo de negócios para desenvolvimento de *software*, proposto pela Sociedade SOFTEX (2002) e apresentado no item 3.4.2.1; o tipo de estratégia competitiva adotada, proposto por Fleury e Fleury (1999), e apresentado no item 4.1.4; o tipo de articulação global, também proposto por Fleury e Fleury (1999), e analisado no item 4.3.3; e a forma de atuação no mercado de segurança, discutida no item 5.3.

Quanto ao **modelo de negócios** de produção de *software*, a empresa Alfa atualmente não pode ser caracterizada. No passado, ela já foi uma companhia de produto/pacote, passando em seguida para um modelo de serviços de alto valor. Já a Beta possui no desenvolvimento de *software* o foco de sua estratégia atual, direcionando-se para o mercado de produtos que possam ser vendidos em todo o mundo, e que requerem grandes esforços em P&D. Em casos específicos, a Beta realiza o desenvolvimento de serviços de alto valor. A Gama possui uma estratégia mais ampla, fazendo desde projetos de baixo valor, tais como consultoria de segurança em sistemas *Web* e análise de código, até *softwares* de alto valor, contratados por clientes

específicos. Dois exemplos de *softwares* de alto valor da empresa atualmente se tornaram produtos.

A classificação da **estratégia competitiva** das empresas deve ser considerada como uma aproximação, já que uma análise mais longa e envolvendo pesquisas com clientes destas empresas seria necessária para apurar devidamente este critério. A Alfa é, das três empresas, a que mais evoluiu em termos de *marketing* e estratégia comercial, tendo como foco as grandes empresas, principalmente do governo. Além disso, a empresa possui várias características de inovação incremental, como, por exemplo, na área de recursos humanos e aprendizagem organizacional. Na sua história, também foram desenvolvidos produtos que se tornaram referência no mercado brasileiro de segurança.

Quanto ao *marketing*, foi possível identificar que os projetos realizados com clientes do governo, principalmente quando possuem um impacto nacional, servem de excelente máquina de propaganda para a empresa. A Alfa possui um grande reconhecimento em todo o país devido ao projeto da segurança das eleições informatizadas, realizado pela empresa. Além disso, esses projetos criam uma rede de relacionamentos bastante grande, tanto no setor público quanto privado, facilitando a entrada da empresa em novos projetos. Esta foi inclusive uma vantagem da Alfa sobre as duas outras, já que o Presidente e outros diretores comerciais da empresa possuem um bom relacionamento com empresários e, principalmente, pessoas públicas, criando assim uma forte rede de contatos para trazer novos negócios à Alfa.

A Beta se propõe, no relato dos seus diretores, a ser uma empresa de inovações radicais, com uma grande valorização da área de P&D. Entretanto, a companhia possui uma carência na área comercial e de *marketing* para conquistar o seu mercado. Já a Gama, com a sua pluralidade de atuação, representa um caso particular de uma empresa de serviços que possui como competência essencial o P&D, desenvolvendo soluções e sistemas específicos, os quais estão sempre ligados a contratos com clientes.

As três empresas estudadas ainda estão mal posicionadas em termos de **articulação global**. A Alfa recebeu dois aportes de capital na sua história, sendo que um deles representou a compra de parte da empresa por uma organização multinacional da área de TI. É importante notar que esta multinacional não é da área de Segurança da Informação, e investiu na Alfa com o objetivo de possuir uma porta de entrada no Brasil, caso o mercado de segurança obtivesse um grande crescimento no futuro. Foi possível notar que, mesmo com um processo de gestão definido e com metodologias

próprias de trabalho, o aporte de capital provocou várias reestruturações na Alfa, tanto em relação às estratégias de mercado, abandono de determinados produtos e serviços e mudanças na organização, tendo como conseqüência o fato de que os sócios diretores agora não possuem mais o controle total da empresa. Devido a isso, classificamos a estratégia de articulação global da empresa como Tipo B.

A classificação da estratégia da Beta como Tipo A deve ser vista com bastante cautela, e entendida mais como uma possibilidade futura, já que os executivos da companhia declararam estar em busca de um novo aporte de capital. Como eles mesmos relataram, as empresas investidoras possuem atualmente interesses em determinados produtos da Beta, e não no mercado de segurança em si. Neste caso, a empresa estaria livre da influência externa do investidor, fornecendo tecnologia de ponta na cadeia produtiva. O primeiro aporte de capital obtido pela Beta foi feito com grupos de investidores nacionais, que, segundo os entrevistados, não interferem na administração da empresa. Os executivos da Beta ainda precisam, entretanto, amadurecer e formalizar os seus processos, além de vencer a grave crise financeira que se abate sobre a companhia. Só então serão capazes de inserir a empresa em parcerias globais.

A Gama se mantém isolada no mercado nacional, sem optar por inserção na cadeia produtiva global. Como foi visto no estudo de caso, os diretores afirmam que ainda existe muito espaço no mercado brasileiro a ser conquistado.

Finalmente, a **atuação no mercado de segurança** por parte das três empresas também é distinta. A Alfa, que praticamente já passou por todos as formas de atuação, desde o desenvolvimento de produtos de segurança, serviços profissionais e desenvolvimento de *software*, atualmente se posiciona como uma integradora, usando a sua experiência no mercado para montar soluções completas para os seus clientes. Os executivos da empresa disseram que a parceria estratégica é vital para que a empresa possa oferecer aos seus clientes as soluções que os mesmos necessitam.

A Beta é a mais radical das três em relação à sua estratégia de mercado, atuando como uma fábrica de produtos de *software*, tipo de atuação descrita no item 5.3.1. Entretanto, a empresa vem enfrentando uma grave crise com essa estratégia, pois não está conseguindo manter-se financeiramente enquanto o mercado não começa a absorver os seus produtos.

A Gama permanece como uma empresa atuando em todas as áreas da segurança, com exceção do desenvolvimento de produtos, a não ser que os mesmos sejam evoluções de *softwares* desenvolvidos para clientes específicos. Os executivos da

empresa optaram por uma postura mais realista, sem um foco específico, mas conseguindo sempre realizar projetos e manter as finanças da firma. O maior problema da empresa é a sua dificuldade em estabelecer parcerias, justamente pela abrangência de atuação muito grande.

As empresas que criaram cursos e treinamentos na área de segurança destacaram este negócio como bastante produtivo, pois é um serviço que exige pouco custo e possui uma grande demanda, principalmente em se tratando de um conhecimento novo e não coberto pelas universidades. Além disso, serve como uma ferramenta de *marketing* da empresa.

Apontar qual das três empresas do estudo de casos foi a mais bem sucedida é uma tarefa difícil, já que as mesmas possuem tempos de atuação no mercado e objetivos distintos. A empresa Alfa, por exemplo, já passou por excelente "saúde financeira", chegou a obter faturamentos anuais perto de R$ 20 milhões e desenvolveu uma marca bastante forte no Brasil. Apesar disso, tem encontrado várias dificuldades com a diminuição das compras feitas pelo governo e por grandes empresas. A sua atuação baseada em soluções de segurança integral também parece estar migrando para grandes empresas, como a IBM, por exemplo, de acordo com as tendências apontadas no item 5.4.3. Tanto a Alfa quanto a Beta são empresas bastante dependentes de clientes específicos: governo e área financeira, respectivamente. A Alfa, inclusive, é a única das três firmas a possuir entrada nos projetos do governo, fruto do seu bom *marketing* e reconhecimento.

O foco em tecnologias com alta barreira de entrada no mercado, estratégia adotada pela Beta, faz bastante sentido, mas se mostra difícil nos tempos de crise atuais e no contexto brasileiro. Devido a isso, mais do que nunca se faz necessário estar preparado para mudanças de rumo e estratégia. No caso da empresa Gama, a falta de foco a torna muito mais vulnerável a empresas concorrentes de serviços de baixa qualidade, como as empresas de redes que dizem prestar serviços de segurança.

7 CONCLUSÕES

O presente estudo teve como objetivo apresentar uma descrição geral do mercado de Segurança da Informação no Brasil e uma análise das empresas atuantes na área. Para isso, fizemos uma apresentação teórica sobre segurança eletrônica, a TI no Brasil e sobre as estratégias empresariais recomendadas para empresas da Nova Economia. A quantidade de assuntos diferentes tratados neste trabalho mostrou-se necessária, devido à diversidade do tema e à novidade da área de Segurança da Informação.

Para complementar o estudo, realizamos uma pesquisa com três empresas localizadas na cidade do Rio de Janeiro, tendo como foco de análise as estratégias competitivas utilizadas pelos executivos dessas companhias e o ambiente local de Tecnologia da Informação em que as mesmas estão inseridas.

O estudo realizado pela Sociedade SOFTEX (2002) e demais informações colhidas a partir de autores tais como Marques (2003), Pacciti (2000), Segre e Rapkiewicz (2003), dentre outros, sobre Tecnologia da Informação no Brasil, em especial o *software*, mostraram-se aplicáveis aos estudos de caso para as empresas de segurança, levando-se em conta o fato de que as três empresas analisadas já estiveram envolvidas com o desenvolvimento de sistemas.

Foi possível confirmar a importância exercida pelo meio acadêmico nas empresas estudadas, todavia, atualmente, esta importância está limitada ao fornecimento de recursos humanos e à criação de uma cultura de TI. Não há uma interação entre as pessoas e as suas universidades de origem, a partir do momento em que se formam, algo que talvez possua uma parcela de culpa tanto das instituições governamentais quanto das empresas. As primeiras pouco incentivam este relacionamento e não estabelecem as condições para um melhor aproveitamento das instituições de ensino, e as últimas atribuem uma prioridade bastante baixa à interação com a universidade.

Para analisar as estratégias competitivas das empresas, fizemos uma classificação aproximada a partir do modelo de Fleury e Fleury (1999), apresentado no item 4.1.4, identificando os principais aspectos focados pelas empresas estudadas, tais como P&D, *marketing*, área comercial, inovação e parcerias estratégicas. A empresa Beta, por exemplo, possui uma boa definição da sua estratégia, focada em produtos do tipo *breakthrought*, mas, em contrapartida, não possui uma estratégia de vendas e

marketing suficientemente madura para conquistar os seus clientes. As outras duas empresas dão maior valor aos serviços e à consultoria, sendo que a Alfa possui um histórico bastante forte em *marketing* e vendas voltadas para um cliente específico, no caso o governo, como já foi analisado no capítulo anterior.

O modelo para estratégias de articulação global, também definido por Fleury e Fleury (1999) e apresentado no item 4.3.3, foi útil para mostrar o quão distantes as empresas brasileiras de segurança ainda estão das corporações mundiais. A única empresa (Alfa) que se articulou com uma multinacional estrangeira fez isso através da venda de grande parte de suas ações. Os resultados dessa estratégia não se mostraram positivos, já que a empresa Alfa tornou-se dependente das decisões do investidor estrangeiro em várias questões, perdendo um pouco da sua autonomia. A empresa Beta parece estar no caminho certo em relação à sua estratégia de inserção global, como vimos no capítulo anterior, mas não existe ainda nada concreto.

Em termos de inovação, o Brasil ainda precisa avançar bastante, principalmente com o amadurecimento da parte gerencial das empresas, e de uma maior colaboração entre as mesmas, de forma a compensar a falta de recursos. Além disso, é essencial um programa governamental com foco em P&D nas empresas, com o objetivo de dar às mesmas o apoio financeiro para a criação e desenvolvimento de produtos. Muitas empresas se dizem inovadoras apenas como uma questão de *marketing*, mas não colocam a inovação como um valor essencial, patrocinado pela diretoria como algo de importância estratégica. É muito comum ver a palavra inovação em *folders*, *sites* e outros meios pelo qual a empresa se apresenta, ou até mesmo nas visões e missões declaradas e estampadas nas paredes da firma. Mas na maioria dos casos, representa mais uma fachada com objetivos de autopromoção no mercado.

A dificuldade na realização de parcerias e redes nacionais de empresas, destacada na pesquisa realizada pela Sociedade SOFTEX (2002) e apresentada no capítulo 3, foi confirmada nos estudos de casos, até mais do que se esperava. Apesar da disposição das firmas e do discurso em prol das parcerias e cooperação, muito pouco foi observado na prática, e este quadro parece pouco provável de obter uma mudança em curto prazo. A forma imediatista de gestão e a falta de unidade entre as empresas, aliada a uma ausência na definição de estratégias de atuação, torna as parcerias, em alguns casos, impossíveis de se efetivarem, fazendo com que as empresas nacionais do setor fiquem vulneráveis frente às multinacionais que cada vez mais atuam no país.

Neste trabalho, também pudemos problematizar alguns conceitos relativos às estratégias competitivas empregadas em países desenvolvidos, quando aplicadas ao Brasil. Na revisão teórica deste estudo, destacamos a necessidade de uma definição de competências essenciais e foco de atuação no mercado para as empresas da chamada Nova Economia. Todavia, nos estudos de casos, foi possível verificar que uma empresa (Beta) que definiu sua competência essencial e foco estritamente na área de *software* está enfrentando grandes dificuldades de sobrevivência no mercado. No Brasil, as empresas acabam por definir um escopo muito grande de atuação, como fez a Gama, para garantir a sobrevivência nos períodos de crise, o que, em contrapartida, dificulta a realização de parcerias. Os fatores particulares que influem na vida das empresas brasileiras precisam ser mais explorados por novos estudos, de forma a complementar os conceitos de estratégias empresariais já existentes.

As barreiras ao desenvolvimento das PMEs no Brasil, analisadas nos itens sobre as pequenas e médias empresas (4.2.3), sobre a competitividade brasileira (4.3.1) e também destacadas na pesquisa feita pela Sociedade SOFTEX (2002), apresentada no item 3.4.2.2, foram confirmadas nos estudos de caso. Questões como altos impostos, tratamento equivalente comparado às multinacionais, excesso de burocracia e custos elevados no processo de abertura e fechamento de empresas e falta de acesso ao capital de risco, público ou privado, foram igualmente citadas pelas empresas do estudo de casos, principalmente pelas menores (Beta e Gama).

Particularmente sobre os impostos, os entrevistados destacaram a importância dos incentivos fiscais concedidos por estados e municípios. O estudo feito pela Sociedade SOFTEX (2002) também levantou (no item 3.4.3) a necessidade de novas políticas governamentais que estimulem estes incentivos fiscais no país. Por exemplo, o ISS (Imposto Sobre Serviços) é de competência dos Municípios e do Distrito Federal, assim como o ICMS (Imposto sobre Circulação de Mercadorias), que incide sobre as exportações, é de competência dos Estados e do Distrito Federal (PORTAL TRIBUTÁRIO, 05 fev. 2004). Diferentes estados e municípios podem fazer uso de incentivos em relação a estes tributos, atraindo novos empreendimentos. Os entrevistados da empresa Gama disseram que os incentivos fiscais da cidade de São Paulo, atualmente, estão mais atraentes que os do Rio de Janeiro.

As empresas também se queixaram bastante do regime de trabalho aplicado a funcionários de TI, que em geral ganham altos salários. De uma certa forma, é compreensível a proposta de flexibilização das regras trabalhistas para estes

profissionais, com o intuito de facilitar a sua contratação e reduzir os custos relativos a impostos para as firmas. Apesar destes serem problemas de qualquer empresa em qualquer ramo, no caso das empresas nacionais de tecnologia, estas questões se mostram mais acentuadas, já que os empresários precisam de muito mais "fôlego financeiro" para investir em novas tecnologias e contar com a sua absorção pelo mercado, o que nem sempre ocorre em curto prazo. Já os impostos incidem mensalmente nas contas das empresas, independente dos lucros (ou prejuízos) obtidos.

Todavia, o contato com funcionários das empresas estudadas mostrou que os mesmos também se queixam da falta de participação nos lucros, em tempos de prosperidade financeira. Se por um lado os empresários querem flexibilizar as leis trabalhistas em tempos de crise, os mesmos não costumam adotar planos de participação nos lucros e resultados nos períodos de sucesso econômico.

Para as políticas de fomento à indústria de tecnologia, é preciso que seja feita uma revisão do que já existe, de forma a contemplar algumas lacunas observadas nos estudos de casos, e que já foram apontadas nos capítulos 3 e 4. Principalmente para o caso das PMEs, categoria das empresas estudadas, La Rovere (1999) sugere a criação de entidades tecnológicas setoriais, que se responsabilizem por:

- Administrar projetos de P&D e de inovação;
- Estimular e promover a transferência de tecnologia às empresas do setor;
- Coordenar laboratórios existentes que forneçam recursos de P&D às firmas;
- Coordenar normas técnicas e desenvolvimento de padrões nacionais;
- Coordenar programas de recursos humanos;
- Organizar bancos de dados em inovações, tecnologia e informações empresariais;
- Coordenar programas de gestão de qualidade;
- Organizar eventos, simpósios e exibições.

Dessa forma, poderiam ser formadas no país, ou até mesmo regionalmente, entidades que agrupassem empresas da área de Segurança da Informação, permitindo às mesmas um auxílio na definição de foco estratégico, evitando a concorrência e incentivando a complementação dos seus serviços. Muitas dessas empresas ainda possuem grandes dificuldades em estabelecer parcerias e, por sua vez, em conquistar clientes maiores, justamente pelas suas dificuldades na definição de estratégias e foco de atuação.

Acreditamos que, através destes grupos empresariais, existe a possibilidade de se fazer frente à concorrência de empresas multinacionais, mesmo contando apenas com PMEs articuladas. Como colocam Marques e Segre (2003, p. 352):

> Se ponderarmos e analisarmos o que faz uma empresa estar ou parecer grande, poderemos talvez mais facilmente arquitetar maneiras de conseguir efeitos de tamanho a partir das redes presentes local, regional ou nacionalmente no Brasil.

Além disso, os programas de fomento precisam claramente inserir essas empresas nos projetos de tecnologia governamentais, facilitando o acesso de novas e pequenas empresas ao capital de risco. O governo brasileiro precisa também comprar mais destas empresas, e não apenas de grandes firmas conhecidas de longa data. Só assim será possível multiplicar o número de PMEs dentro do país.

Um exemplo de novas políticas que estão sendo definidas é a "Lei de Inovação Tecnológica", que visa viabilizar projetos de pesquisa. De acordo com Cruz (2003), a lei vem trazer ao Brasil o resultado de um consenso que há muito tempo existe nos países desenvolvidos, de que o "poder de compra do Estado é um dos motores que viabiliza a atividade inovativa" (CRUZ, 07 ago. 2003). O autor chama este instrumento de "encomendas tecnológicas", através do qual o "Estado, em vez de comprar indiscriminadamente a partir do menor preço internacional, faz a opção pelo desenvolvimento do produto numa empresa nacional" (CRUZ, 07 ago. 2003).

Essa estratégia já foi largamente utilizada pelos Estados Unidos, Europa e Japão, com bastante sucesso. Por exemplo, é a principal maneira pela qual o Estado apóia o desenvolvimento de Ciência e Tecnologia nos Estados Unidos, com cerca de US$ 20 bilhões de dólares anuais gastos em compras tecnológicas pelas agências governamentais do país. Nas palavras de Cruz, "o valor da compra pode até sair mais caro, num primeiro momento, mas o ganho com a detenção do conhecimento e com o domínio tecnológico daí resultante é altamente compensador" (CRUZ, 07 ago. 2003).

As incubadoras de empresas também têm se mostrado uma excelente opção para novas empresas, diminuindo o chamado "Custo Brasil" que tanto bloqueia o desenvolvimento das firmas. Já existem vários casos de sucesso de empresas de tecnologia incubadas em universidades brasileiras, como, por exemplo, a PUC do Rio de Janeiro e a UFRJ.

As empresas brasileiras de segurança, assim como as empresas que não queriam entrar na competição dos fabricantes de minicomputadores nos anos 1970, não possuem

estrutura para enfrentar um mercado global. Neste ponto, instituições como o BNDES poderiam se tornar importantes agentes para o apoio financeiro, tão necessário à P&D e à exportação, ajudando a criar uma credibilidade para a tecnologia nacional.

Em relação ao mercado de Segurança da Informação, os resultados obtidos neste estudo não correspondem totalmente a algumas de nossas expectativas. Quando iniciamos a pesquisa, partimos do pressuposto de que o mercado para a área de segurança estava em crescimento constante no Brasil e no mundo, o que influenciou a escolha do tema. Porém, as conversas com alguns executivos das empresas estudadas e a leitura de diversos artigos em mídias especializadas mostraram tendências bem menos otimistas. É um fato que as questões relativas à Segurança da Informação serão cada vez mais importantes em todo o mundo, como citou Yourdon (2002), principalmente após os trágicos eventos que marcaram o mundo após 11 de setembro de 2001 e devido às constantes disseminações de vírus de computador por todo o planeta. Entretanto, o futuro do que poderia ser chamado de "Mercado de Segurança da Informação" é uma incógnita.

Segundo vários especialistas da área e os entrevistados nos estudos de casos, o mercado de consultoria em segurança tende a desaparecer, com a segurança transformando-se em um componente embarcado de outras tecnologias. Como colocou um dos entrevistados, "no futuro iremos comprar produtos tecnológicos, tais como computadores ou telefones celulares, que trarão uma espécie de selo de segurança". Ou seja, por trás deste selo, estará embutida toda uma tecnologia de segurança que, no entanto, será invisível para o consumidor. Uma outra tendência que também foi citada são os grandes provedores de serviços de segurança e os *Data Centers*, que cada vez mais terão um papel de destaque, ao centralizar os servidores corporativos dos seus clientes, juntamente com os *softwares* necessários. Estes provedores também estarão encarregados dos serviços de segurança, assumindo o papel das atuais empresas de Segurança da Informação.

Essas duas tendências, entretanto, só vêm reforçar a importância da atividade de desenvolvimento de *software* de segurança, que foi uma das premissas que assumimos na introdução deste estudo. Esta atividade parece ser uma boa oportunidade de investimento para as empresas de *software* brasileiras, pelas seguintes razões:

- Sistemas de segurança possuem um alto valor agregado em conhecimento, pois envolvem tecnologia de ponta que requer grande capacitação de recursos humanos no país;

- *Software* embarcado em outras tecnologias possui grande retorno financeiro, devido ao elevado número de unidades vendidas;
- *Software* embarcado é potencialmente um líder de exportações mundiais;
- Devido aos altos salários cobrados por desenvolvedores de *software* em países desenvolvidos, principalmente em áreas que requerem grande nível de capacitação, o Brasil tende a se tornar um alvo para empresas interessadas em *outsourcing* especializado.

Mais do que nunca, é preciso que o Governo brasileiro trate a questão do *software* nacional e da competitividade das empresas que o desenvolvem como sendo prioritária na área de Tecnologia da Informação, para que possamos nos inserir no mercado de *software* mundial voltado para Segurança da Informação, enquanto ainda é tempo.

Por se tratar de um tema bastante amplo e com várias questões que ainda estão em processo de definição, colocamos a seguir algumas sugestões para trabalhos futuros. Poderiam ser realizadas pesquisas:

- com estudos de casos, utilizando a mesma metodologia desta, porém tendo como foco empresas de Segurança da Informação da cidade de São Paulo;
- com estudos de casos, com a mesma metodologia, mas focando um outro segmento da Tecnologia da Informação, o qual também possua o desenvolvimento de *software* como um fator diferencial;
- comparando o mercado brasileiro de Segurança da Informação com o de outro país que possua condições parecidas de desenvolvimento[13], tal como a Irlanda ou Israel;
- com empresas clientes de um determinado segmento, como o governo, de forma a avaliar melhor as necessidades de Segurança da Informação existentes nestas organizações e o que as mesmas esperam das empresas prestadoras de serviços nesta área.

[13] De acordo com a pesquisa feita pela Sociedade SOFTEX (2002), o Brasil se encontra em situação bastante parecida com a desses países no que diz respeito ao potencial para desenvolvimento de *software*.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, A. L. *Comércio Eletrônico: Modelo, aspectos e contribuições de sua aplicação.* São Paulo: Atlas, 1999.

ALBUQUERQUE, R. e RIBEIRO, B. *Segurança no Desenvolvimento de Software.* Rio de Janeiro: Campus, 2002.

ALMEIDA, A. L. V. C. *Comércio Eletrônico na Relação Inter-Empresarial da Administração Pública: Um Estudo de Caso no Governo Federal.* Tese de M.Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2000.

BRINEY, A. "The Influence List: The vendors, Technologies and people that shaped our past and frame our future". *Security Magazine*, November 2002. Disponível em <http://infosecuritymag.techtarget.com/2002/nov/influence.shtml>. Acesso em: 25 jan. 2004.

BUSTAMANTE, J. *Brazil B2B and eMarketplaces – Brazil Internet Data Center Market and Trends*, 2001. IDC BR1236, v.1, May 2001.

CASTELLS, M. *A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura.* São Paulo: Ed. Paz e Terra, v. 1, 1999.

CERIONI, T. A. "Boas Perspectivas para o Mercado de Data Center no Brasil". *IT Mídia Ltda,* 29 jan. 2003. Disponível em: <http://www.telecomweb.com.br/noticias/artigo.asp?id=34414>. Acesso em: 19 dez. 2003.

CESAR, R. "Empresas de segurança investem no Brasil". *ComputerWorld*, set. 2003. Disponível em <http://www.computerworld.com.br/AdPortalV3/adCmsDocumentoShow.aspx?Documento=23364>. Acesso em: 19 jan. 2004.

COSTABILE, H. e AZEVEDO, L. M. "Os Bancos no Futuro e o Papel da Tecnologia". In: *CIAB2003/FEBRABAN,* jun. 2003, São Paulo. *Resumo dos trabalhos.* São Paulo: [s.n.], 2003.

CRUZ, C. H. B. "O poder de compra do Estado: Lei de Inovação Tecnológica Pode Viabilizar Projetos de Pesquisa". *Gabinete do Reitor – UNICAMP*, Campinas, 2003. Disponível em <http://www.gr.unicamp.br/artigos/artigo_Poder_de_compra_do_Estado.htm>. Acesso em 07 ago. 2003.

EDWARDS, S. "Information technology and economic growth in the emerging economies". *University of California*, Los Angeles, 2001. Disponível em <http://www.anderson.ucla.edu/faculty/sebastian.edwards/papers.htm>. Acesso em 24 ago. 2003.

FÁVARO, T. "Ex-alunos transformam-se em empresários". *Correio Popular*, Campinas, 04 out. 2003. Disponível em <http://www.cosmo.com.br/hotsites/cenarioxxi/2003/10/04/materia_cen_67243.shtm>. Acesso em 20 fev. 2004.

FERNANDES, A. "E-Governo no Brasil". Brasília: *SF/BNDES*, 2001 Disponível em <http://www.federativo.bndes.gov.br>. Acesso em 18 set. 2003.

FLEURY, A. e FLEURY, M. T. L. *Aprendizagem e Inovação Organizacional: As Experiências de Japão, Coréia e Brasil*. São Paulo: Atlas, 1997.

FLEURY, A, FLEURY, M. T. L. *Estratégias Empresariais e Formação de Competências: Um Quebra-cabeça Caleidoscópico da Indústria Brasileira*. São Paulo: Atlas, 1999.

HUNT, S. "Market Overview: Managed Security Services". Planning Assumption, RPA-042001-00020, *Giga Information Group*, Apr. 2001. Disponível em <www.counterpane.com/giga3.pdf>. Acesso em 16 jan. 2004.

INTERNATIONAL DATA CORPORATION. "Análise de Mercado. Brazil Internet Data Centers Market and Trends", 2002. São Paulo: *IDC Brasil*, #BR1405, v. 1, out. 2002.

LA ROVERE, R. "As Pequenas e Médias Empresas na Economia do Conhecimento: implicações para políticas de inovação". In: LASTRES, H. M. M. e ALBAGLI, S., *Informação e Globalização na Era do Conhecimento*. Rio de Janeiro: Campus, 1999, pp. 145-163.

LEMOS, C. R. "Inovação na Era do Conhecimento". In: LASTRES, H. M. M. e ALBAGLI, S., *Informação e Globalização na Era do Conhecimento*. Rio de Janeiro: Campus, 1999, pp. 122-144.

LIMA, M. I. S. *Terceirização em informática: Análise das motivações e impactos baseada em estudos de casos*. Tese de M.Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 1996.

LONEEF, D. "Os pilares da segurança". *Revista e-Manager*, São Paulo, n. 39, pp. 20-23, maio 2003.

LUNARDI, G. L., BECKER, J. L. e MAÇADA, A. C. G. "A Tecnologia de Informação (TI) como Ferramenta Estratégica nos Bancos do CONESUL". In: *XXI Encontro Nacional de Engenharia de Produção*, Salvador: out. 2001.

MALDONADO, J. "Tecno-globalismo e Acesso ao Conhecimento". In: LASTRES, H. M. M. e ALBAGLI, S., *Informação e Globalização na Era do Conhecimento*. Rio de Janeiro: Campus, 1999, pp. 105-121.

MARQUES, I. C., "Minicomputadores brasileiros nos anos 1970: uma reserva de mercado democrática em meio ao autoritarismo". *História, Ciências, Saúde - Manguinhos*, vol. 10(2), pp. 657-81, maio-ago 2003.

MARQUES, I. C. e SEGRE, L. M. "Problematizando o tamanho das empresas: a multiplicidade do 'grande' e do 'pequeno' na sociedade em rede". In: LASTRES, H. M. M., CASSIOLATO, J. E. e MACIEL, M. L., *Pequena Empresa: Cooperação e Desenvolvimento Local*. Rio de Janeiro: Relume Dumará, 2003, pp. 347-363.

MENEZES, C. E. "Você compraria um software brasileiro?" *Agência Estado Setorial*. 20 maio 2003. Disponível em: http://www.aesetorial.com.br/tecnologia/artigos/2003/mai/20/198.htm. Acesso em 20 set. 2003.

OLIVEIRA, E. T. "Hospedagem Cinco estrelas". *World Telecom*, São Paulo: IDG Computerworld do Brasil Serviços e Publicações, a. 3, n. 29, p. 6, dez. 2000.

PACCITI, T. *Do FORTRAN à Internet: No rastro da trilogia educação, pesquisa e desenvolvimento*. São Paulo: Makron Books, 2000.

PASSOS, C. A. K. "Novos Modelos de Gestão e as Informações". In: LASTRES, H. M. M. e ALBAGLI, S., *Informação e Globalização na Era do Conhecimento*. Rio de Janeiro: Campus, 1999, pp. 58-83.

PINTO, S. L. e SANTANA, A. M. "Proposta de Política de Governo Eletrônico para o Poder Executivo Federal". *Grupo de Trabalho Novas Formas Eletrônicas de Interação*. Brasília, 2000. Disponível em <http://www.governoeletronico.gov.br/arquivos/proposta_de_politica_de_governo_eletronico.pdf>. Acesso em 20 mar. 2003.

PUTTINI, R. S. "Criptografia e Segurança de Redes de Computadores". *Mestrado em Engenharia de Redes e Tecnologias da Informação*. UnB – Departamento de Engenharia Elétrica, 2000. *Material eletrônico do curso*. Disponível em <http://webserver.redes.unb.br/security/seguranca.htm>. Acesso em 15 ago. 2003.

ROBERTS, P. "Security market to hit $45 billion by 2006". *InfoWorld*, 04 fev. 2003. Disponível em <http://www.infoworld.com/article/03/02/04/HNsecure_1.html>. Acesso em 17 ago. 2003.

ROSE, T. "Fomento ao Desenvolvimento do Software Educacional". In: *Educação em Bytes '96*, ago. 1996. Disponível em <http://www.cciencia.ufrj.br/Publicacoes/Artigos/EduBytes96/FomentoSoftEduc1.htm>. Acesso em 07 jan. 2004.

SCHNEIER, B. "Managed Security Monitoring: Network Security for the 21st Century". *Counterplane Internet Security, Inc.*, 2001. Disponível em <http://www.counterpane.com/literature.html>. Acesso em 20 jan. 2004.

SCHWARTZ, M. "Trust but Verify". *Computerworld*, 12 fev. 2001. Disponível em <http://www.computerworld.com/printthis/2001/0,4814,57532,00.html>. Acesso em 30 jan. 2004.

SEGRE, L. M. e RAPKIEWICZ, C. E. "Mercado de trabajo y formación de recursos humanos em tecnologia de la información em Brasil. ¿Encuentro o desencuentro?" In: LABARCA, G., *Reformas econômicas y formación*. Montevideo: CINTERFOR, 2003, pp. 211-264.

SOARES, E. "Volta por Cima, Especial – Data Centers". *RNT - Revista de Negócios em Telecomunicações*, São Paulo: Advanstar Editora e Comunicações, ano 24, n.280, p.34, dez. 2002.

SOCIEDADE SOFTEX. "A Indústria de Software no Brasil – 2002: Fortalecendo a Economia do Conhecimento". In: *Slicing the knowledge-Based Economy (KBE) in India, China and Brazil: a tale of three software industries*. Massachussets Institute of Technology – MIT, 2002; Brasil Coordenação geral Sociedade SOFTEX. – Campinas, 2002, 80 p.

TANENBAUM, A. S. *Redes de Computadores*. Tradução da 3a Edição. Rio de Janeiro: Campus, 1997.

TIGRE, P. B. "Comércio Eletrônico e Globalização: Desafios para o Brasil". In: LASTRES, H. M. M. e ALBAGLI, S., *Informação e Globalização na Era do Conhecimento*. Rio de Janeiro: Campus, 1999, pp. 84-104.

TIGRE, P. B. *Computadores Brasileiros: Indústria, Tecnologia e Dependência*. Rio de Janeiro: Campus, 1984.

TIGRE, P. B. "Mitos e Realidades sobre a Difusão do Comércio Eletrônico nas Empresas Brasileiras". In: *Globalization and E-Commerce. Center for Research on Information Technology and Organization* (CRITO), Universidade da Califórnia em Irvine, 2003.

TUESDAY, V. "Security Outsourcing: Don't Bet on It – Yet". *Computerworld*. 11 jun. 2001. Disponível em <http://www.computerworld.com/securitytopics/security/story/0,10801,61232,00.html>. Acesso em 30 jan. 2004.

VILARIM, G. O. *Inovação e Recursos Humanos: Um Estudo de Caso em Empresas de Informática do Rio de Janeiro*. Tese de M.Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2002.

VILLELA, A. V., SUZIGAN, W. *Elementos para a discussão de uma política industrial no Brasil*. Brasília: IPEA, 1996. (Texto para Discussão nº 421).

YOURDON, E. *Byte Wars: The Impact of September 11 on Information Technology.* Prentice Hall PTR, 2002.

REFERÊNCIAS COMPLEMENTARES

Livros

DJANKOV S., LA PORTA, R., DE SILANES, F. L., SHLEIFER, A. "The regulation of Entry". *National Bureau of Economic Research. Working Paper 7892.* Harvard University, 2000.

HAMMER, M. *The Agenda: What Every Business Must Do to Dominate the Decade.* Crown Business, 2001.

MYLOTT III, T. R. *Computer Outsourcing: Managing the transfer of computer systems.* Prentice Hall, 1995.

Textos na Internet

CSO ONLINE. *Brasil é o segundo país mais atacado por hackers.* 17 fev. 2003. Disponível em <http://www.csoonline.com.br/AdPortalV3/adCmsDocumentoShow.aspx?Documento=22348>. Acesso em: 07 jul. 2003.

FEBRABAN. *O Setor Bancário em Números,* 2003. Disponível em <http://www.febraban.org.br/ ciab05/port/dados/conteudo.htm>. Acesso em: 26 jan. 2004.

FINANSOFT. *Uso de Linhas de Financiamento por Empresas de Software no Brasil.* Disponível em <http://www.finansoft.com.br/fin_estatisticas.html>. Acesso em: 10 jan. 2004.

ICP-BRASIL. *Perguntas* Freqüentes *(F.A.C) - Certisign,* 2003. Disponível em <http://www.certisign.com.br/ icpbrasil/faq.html>. Acesso em: 17 out. 2003.

PORTAL TRIBUTÁRIO. *Os Tributos no Brasil.* Disponível em <http://www.portaltributario.com.br/tributos.htm>. Acesso em: 05 fev. 2004.

SIIA. "Information Security Trade Mission to Europe". *Software Information Industry Association,* 2002. Disponível em <http://www.siia.net/divisions/global/trademissions/tmparis/overview.pdf>. Acesso em: 20 jul. 2003.

TELECOM GLOSSARY. *Glossary of Telecommunication Terms*, 2000. Disponível em <http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm>. Acesso em: 25 jan. 2004.

Periódicos

Revista e-Manager

Sites na Internet

Acompanhamento Profissional do Ex-aluno
http://www.dcc.ufrj.br/~exalunos/principal.htm - Acesso em: 19 jan. 2004.

ASSESPRO
http://www.assespro.org.br/ - Acesso em: 01 mar. 2004.

ComputerWorld
http://www.computerworld.com.br - Acesso em: 14 jan. 2004.

CSO Online
http://www.csoonline.com.br - Acesso em: 20 jan. 2004.

Encyclopedia of Computer Security, The
http://www.itsecurity.com/ - Acesso em: 20 dez. 2003.

FEBRABAN
http://www.febraban.com.br/ - Acesso em: 20 nov. 2003.

IBICT – Teses
http://www.ct.ibict.br:81/site/owa/si_consulta - Acesso em: 02 dez. 2003.

IDC Brasil
http://www.idclatin.com/brasil/ - Acesso em: 19 fev. 2004.

Information Security Magazine
http://www.infosecuritymag.com/ - Acesso em: 04 fev. 2004.

MCT – Ministério da Ciência e Tecnologia
http://www.mct.gov.br/ - Acesso em: 19 fev. 2004.

Periódicos CAPES
http://www.periodicos.capes.gov.br/ - Acesso em: 16 nov. 2003.

Portal Tributário
http://www.portaltributario.com.br - Acesso em: 05 fev. 2004.

SOFTEX
http://www.softex.br/ - Acesso em: 20 jan. 2004.

WhatIs.com
http://whatis.techtarget.com/ - Acesso em: 06 fev. 2004.

Wikipedia
http://en.wikipedia.org/ - Acesso em: 28 fev. 2004.

ANEXO I - GLOSSÁRIO

Autoridade Certificadora (AC) – Autoridade na rede que emite e gerencia credenciais de segurança e chaves públicas, para a criptografia de mensagens. Como parte de uma infra-estrutura de PKI, uma AC verifica com alguma autoridade de registro (AR) as informações fornecidas pelo requerente de um certificado digital, para saber se pode ou não emitir o certificado.

Autoridade de Registro (AR) – Autoridade na rede que verifica as requisições de usuários por certificados digitais, e informa a autoridade certificadora se a mesma pode ou não emitir o certificado.

Biometria – Em TI, refere-se a tecnologias utilizadas para medição e análise de características do corpo humano, tais como impressões digitais, íris e retina ocular, padrões de voz e face, dentre outras, com propósitos de autenticação.

Carimbo de tempo (*time stamp*) – Intervalo de tempo de um evento, registrado por um computador. Este intervalo possui medidas apuradas, calibradas em frações de segundos. Com a utilização de tecnologia de certificação digital, esses intervalos podem ser assinados por autoridades reconhecidas, garantindo ainda mais autenticidade dos mesmos.

Certificado digital – Forma de identificação eletrônica que certifica as credenciais de um indivíduo ou sistema durante a realização de transações pela *Web*. É emitido por uma Autoridade Certificadora (AC), e contém o nome, número de série, data de expiração, cópia da chave pública do proprietário e assinatura digital da AC, de forma que a outra parte da transação possa verificar o certificado como real.

Chave pública – Valor fornecido, por alguma autoridade designada, como chave de criptografia que, combinado com uma chave privada, pode ser usado para criptografar mensagens e assinaturas digitais.

Capability Maturity Model (CMM) – Metodologia utilizada para desenvolver e refinar um processo de desenvolvimento de *software* de uma organização. O modelo descreve um caminho evolutivo com cinco níveis, baseados em um aumento da organização e maturidade.

Firewall – Dispositivo para a proteção contra invasões de *hackers* ou transmissões não autorizadas de dados. Existe na forma de *software* e *hardware*, ou na combinação de ambos. O modelo a ser instalado depende do tamanho da rede, da complexidade das

regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.

Freeware – Programas oferecidos a custo zero, e costumam estar disponíveis para *download* e uso na maioria dos sistemas operacionais. Apesar disso, essas aplicações são registradas, e não podem ser reutilizadas em outros programas sem a devida permissão.

Hacker – Termo usado para se referir a um "programador esperto" ou alguém que tenta "quebrar" sistemas computacionais. Normalmente, estas pessoas são programadores ou engenheiros com conhecimentos técnicos suficientes para compreender os pontos fracos dos sistemas.

HSM – Sigla para *Hardware Security Module*, e designa um dispositivo de *hardware* dedicado ao armazenamento de chaves de criptografia. Este dispositivo contém mecanismos de proteção e de falha segura, destruindo as informações armazenadas em caso de tentativas de violação.

Login – Identificação do usuário em um sistema operacional ou aplicação, composto de caracteres.

NASDAQ – Sigla para *National Association of Securities Dealers Automated Quotations*, e designa o primeiro mercado de ações eletrônico da história, que começou suas atividades em 1971. Atualmente, corresponde ao maior mercado de ações eletrônico do mundo, com aproximadamente 3.600 empresas.

Open source – Em geral, se refere a qualquer programa cujo código fonte é colocado à disposição para uso ou modificação da comunidade de usuários.

Public Key Infrastructure (PKI) – Sistema que permite a usuários de uma rede pública e insegura, tal como a Internet, trocar dados e valores monetários de forma segura e privada, através do uso de um par de chaves (pública e privada) de criptografia, obtidos e compartilhados através de uma autoridade confiável.

Security Officer – Termo em inglês usado para se referir à pessoa responsável por todas as questões relativas à Segurança da Informação em uma companhia.

Smart card – Cartão de plástico, nas dimensões de um cartão de crédito, contendo um *microchip* que pode ser carregado com dados, utilizado para ligações telefônicas, pagamentos eletrônicos e outras aplicações. Pode também ser usado para o armazenamento de chaves de criptografia.

Spam – *E-mail* não solicitado na Internet, e costuma funcionar como mala-direta.

Token – Dispositivo pequeno de *hardware* para autorização de acesso em redes, que pode ser carregado como um chaveiro. Em geral, possui as mesmas funcionalidades de um *smart card.*

Virtual Private Network (VPN) – Forma de se usar uma infra-estrutura de telecomunicações pública, tal como a Internet, com o objetivo de prover a escritórios ou usuários individuais remotos um acesso seguro a suas redes corporativas. Uma VPN pode ser contrastada com um caro sistema de linhas privadas que só podem ser usadas por uma única organização. O objetivo da VPN é prover a organização com as mesmas capacidades, porém a um custo bem menor.

Web service – Também conhecido como *application service*, são serviços disponibilizados em um *Web Server* corporativo, para usuários ou demais programas conectados via *Web*.

ANEXO II – GUIA DE ENTREVISTAS

Questões para análise das empresas de segurança

Caracterização da empresa:

- Descrição de produtos e serviços.
- Organograma.
- Missão, visão e foco.
- Número de funcionários.
- Faturamento anual.
- Escritórios e filiais.

Histórico e evolução:

- Como a empresa foi formada?
- Qual era o objetivo inicial?
- Quem teve a idéia de formar?
- Qual era o tamanho inicial da empresa?
- Como a empresa evoluiu ao longo do tempo (marcos)?

Negócio

- Que produtos e serviços a empresa oferece?
- Qual o percentual de produtos nas vendas?
- Qual o percentual de serviços nas vendas?
- A empresa exporta?
- O Softex ou outro programa do gênero influencia?
- Houve mudança recente no negócio?

Inovação

- Para a empresa, o que é inovação?
- O mercado considera a empresa inovadora?
- A empresa se considera inovadora? Em que ponto?
- Existe P&D? Qual o percentual de investimento?
- Como o conhecimento é administrado na empresa?
- Qual o relacionamento entre P&D e *marketing*?
- Quais as tecnologias utilizadas na empresa?
- Existem patentes registradas?

Organização

- Como é a estrutura organizacional da empresa?
- Houve mudança organizacional recente?

- Que mudanças ocorreram devido ao mercado e à concorrência?
- Como é o fluxo de trabalho? Possui metodologias próprias?
- A empresa tem ligação com outros grupos empresariais?
- Existiram investimentos externos ou fusões?
- Quais as dificuldades em se ter uma empresa pequena/média no Brasil?

RH

- Como e onde os profissionais são recrutados e selecionados?
- Os conhecimentos adquiridos em instituições de ensino superior são explorados?
- A empresa valoriza a educação continuada?
- Existe investimento em treinamentos?
- Como são os contratos de trabalho?
- Existe terceirização/subcontratação?
- Os funcionários são alocados por projeto ou funções fixas?
- Existe alocação de h/h?
- Quais as competências essenciais requeridas na empresa?

TI no Brasil

- Existem contatos com outras empresas?
- Quais os canais de ligação com instituições de ensino?
- Qual a sua visão a respeito das empresas brasileiras de TI?
- De que maneira você acha que o governo poderia ajudar a sua e outras empresas do ramo?
- Vocês possuem certificações de qualidade na área de execução de projetos?
- A sua empresa desenvolve *software*? Qual a importância do *software* dentro dos objetivos estratégicos da sua empresa?
- Vocês possuem alguma certificação na área de qualidade de *software*? E qual a sua visão a respeito dessas certificações?
- Como você vê o potencial brasileiro para o desenvolvimento de *software*?
- Você considera que possuímos profissionais capacitados nesta área?

Clientes

- Quem são os clientes da empresa? Qual o perfil?
- Existe feedback do cliente quanto ao produto/serviço?
- Como vocês vêem os DataCenters/MSSPs? Existe alguma idéia de parceria com eles?
- Como vocês vêem a terceirização da segurança pelas empresas em geral? Vocês possuem alguma solução para terceirização de segurança, para os seus clientes?

Mercado

- Qual o foco (ou parcela) de mercado? (Redes, *e-gov*, *e-commerce*, *e-banking*, etc.)
- Possuem soluções ou discursos de mercado específicos para cada um desses segmentos?

- De que maneira as políticas governamentais interferem no mercado de segurança?
- Como vocês vêem a crise atual do mercado de TI, em especial o de segurança, no mundo e no Brasil? De que forma vocês estão enfrentando isso?
- Como você caracteriza o mercado de segurança atualmente no mundo? E no Brasil?
- Você poderia falar sobre as principais mudanças e tendências que ocorreram neste mercado nos últimos anos?
- Como você caracterizaria os principais tipos de produtos, serviços e soluções de segurança?
- Quais as tendências futuras que você vê neste mercado para o mundo e para o Brasil?

Estratégias

- Fale sobre as estratégias empresariais e comerciais utilizadas por vocês.
- Vocês atuam na economia do conhecimento. De que maneira isso influencia a forma como é administrada a sua empresa; e o posicionamento de vocês no mercado?
- Qual a importância do *marketing* na sua empresa? O que vocês possuem nesta área (Internet, departamento, folders, eventos, propagandas em revista, etc.)?