UNIVERSIDADE FEDERAL DO PARANÁ

FABIO ALVES DA SILVA

A EVOLUÇÃO DAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO A PARTIR DAS DEMANDAS DO SETOR FINANCEIRO

CURITIBA

2014

FABIO ALVES DA SILVA

A EVOLUÇÃO DAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO A PARTIR DAS DEMANDAS DO SETOR FINANCEIRO

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Desenvolvimento Econômico, no curso de Pós-Graduação em Desenvolvimento Econômico do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.

Orientador: Prof. Dr. Flávio de Oliveira Gonçalves

CURITIBA

2014

TERMO DE APROVAÇÃO

FABIO ALVES DA SILVA

"A EVOLUÇÃO DAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO A PARTIR DAS DEMANDAS DO SETOR FINANCEIRO"

DISSERTAÇÃO APROVADA COMO REQUISITO PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE NO PROGRAMA DE PÓS-GRADUAÇÃO EM DESENVOLVIMENTO ECONÔMICO DA UNIVERSIDADE FEDERAL DO PARANÁ, PELA SEGUINTE BANCA EXAMINADORA:

Prof. Dr. Flavio de Oliveira Gonçalves
(Orientador/UFPR)

Prof. Dr. Armando João Dalla Costa
(Examinador/UFPR)

Profª Drª Vanessa Ishikawa Rasoto
(Examinador/EXTERNO)

05 de dezembro de 2014

À minha querida esposa Sara e minha filha Rafaela.

AGRADECIMENTOS

Agradeço especialmente à minha querida esposa, Sara, pelo apoio e carinho e imensa dedicação na tarefa de me incentivar incansavelmente a não desistir dos meus sonhos.

À minha filha, Rafaela, fonte de inspiração para resistir aos momentos mais difíceis.

Aos meus pais, que sempre incentivaram meus estudos.

À minha família e aos amigos pelo apoio e pela compreensão nos momentos de ausência.

Aos professores membros das bancas de qualificação e defesa, Armando Dalla Costa, José Guilherme e Vanessa Rasoto, pelas importantes contribuições para elaboração do trabalho.

Aos demais colegas, professores e funcionários da UFPR que me auxiliaram nessa jornada, especialmente, Jeferson, Fabiano, Luciano, Claudi, Jonas, Evandro, Maricélia, Reinaldo, Danilo e Áurea, pela intensa troca de experiências, ensinamentos e atenção.

Agradeço aos colegas do mestrado acadêmico, pelo suporte e paciência nas reuniões de orientação em grupo.

Em especial ao meu orientador, Prof. Dr. Flávio Gonçalves, pelo suporte, paciência e incentivo em todo programa do mestrado.

A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original.

Albert Einstein

RESUMO

O presente trabalho busca apresentar a evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro. A partir de uma abordagem baseada em teorias neo-schumpeterianas, o estudo proporciona uma interpretação das propriedades do mercado de segurança da informação à luz dos regimes tecnológicos, especialmente discutidos por Malerba e Orsenigo (1997; 2007), tornando assim, possível identificar as condições estruturais fundamentais que definem as competências necessárias, os incentivos e as propriedades dinâmicas do processo inovativo do setor. Além disso, o estudo apresenta as trajetórias tecnológicas do setor de segurança da informação, a partir da abordagem de Dosi (1982). Dessa forma, o trabalho descreve como a atividade inovativa no mercado de segurança da informação tem sido orientada por demandas do setor financeiro no desenvolvimento de novas tecnologias para combater as ameaças no mundo cibernético, observando os aspectos de *demand-pull,* definidos por Dosi (1982).

Palavras chave: Segurança da Informação. Setor Financeiro. Regimes Tecnológicos. *Demand-Pull.*

ABSTRACT

This study aims to present the evolution of information security technologies based on from the demands of the financial sector. From an approach based on neo-Schumpeterian theories, the study provides an interpretation of the properties of security information market through of technological regimes, especially discussed by Malerba and Orsenigo (1997; 2007), making it possible to identify the fundamental structural conditions which define the necessary skills, incentives and the dynamic properties of the innovative sector process In addition, the study presents the technological trajectories of the information security industry based on Dosi (1982) approach. Thus the work describes how the innovative activity in the information security market has been driven by demands of the financial sector in the development of new technologies against these threats in the cyber world, observing aspects of demand-pull in Dosi (1982)

Key-words: Information Security. Financial sector. Technological Regimes. Demand-Pull

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Cada vez mais as organizações operam em um mundo rápido e complexo devido principalmente às mudanças no âmbito das tecnologias da comunicação. Atualmente cerca de três bilhões de pessoas conectadas à Internet através de diferentes dispositivos. Pessoas que estão aplicando boa parte do seu tempo online, comprando coisas, se comunicando, trabalhando e se entretendo através da internet.

As tecnologias de informação e comunicação (TICs) constituem um setor de crescente importância econômica. De modo geral, as TICs abrem novas janelas de oportunidades para as organizações, caracterizadas pela possibilidade de criação de novos modelos de negócios e de aumento de produtividade e eficiência. Conforme Tigre e Noronha (2013), diferente de outras tecnologias específicas, aplicadas em processos particulares, as inovações, que surgem a partir do uso das TICs, possuem a característica de transpor, potencialmente, toda a cadeia produtiva.

A evolução das TICs dos últimos 50 anos permitiu a humanidade experimentar significativa redução das limitações de tempo e o rompimento de barreiras geográficas e políticas. As novas tecnologias de informação e comunicação em termos de conceitos, técnicas, políticas, e estratégias alteraram a estrutura competitiva local e global de forma significativa, assim como transformaram as condições de financiamento das atividades da economia, do funcionamento dos mercados financeiros e criaram novas configurações organizacionais.

Esse rápido desenvolvimento das tecnologias de informação e comunicação trouxe consigo o desafio do aumento da complexidade e a evolução das questões relacionadas à segurança da informação. A proliferação dos aparelhos e das redes móveis na última década, a fronteira tênue entre o uso profissional e pessoal dos dispositivos somados aos avançados mecanismos de ataques às redes tornaram imprescindíveis a revisão das estratégias de segurança de informação e das políticas de riscos das organizações.

O aumento vertiginoso do volume de transação de dados e de transações financeiras chama a atenção não somente de quem vê oportunidades para empreender no mundo virtual, mas também de pessoas e organizações mal intencionadas. Para fazer frente a esse cenário, o mercado global de segurança da informação mo-

vimentou 65 bilhões de dólares em 2013 segundo (GARTNER, 2014). O surgimento de inovações no meio virtual tem exigido o desenvolvimento de novos produtos e serviços de apoio na detecção de ataques e invasores.

Diante disto, o entendimento de que a segurança da informação tornou-se uma forma de agregar valor para as organizações tem ganhado a atenção das lideranças das grandes corporações.

Nos últimos 50 anos as TICs deixaram o papel de recurso acessório, e tornaram-se o alicerce dos modelos de negócios que compõem o setor financeiro. Assim, administrar as TICs passou a fazer parte da rotina de tomada de decisão nas organizações. Os mercados financeiros tiveram suas fronteiras ampliadas por meio da interação e da interdependência dos mercados de fatores. Ao passo que as tecnologias de informação e comunicação se proliferaram, o mercado global aumentou de tamanho e em consequência disso, aumentaram os riscos e crises financeiras decorrentes de desequilíbrios de capitais (FONSECA, MEIRELES E DINIZ, 2010).

Com o aumento da variedade dos riscos aumenta também a responsabilidade do setor em evitar o sucesso das fraudes eletrônicas exigindo soluções mais complexas e de alto custo. Os gastos e investimentos são dirigidos para o desenvolvimento de mecanismos de segurança de informação definidos como processos e técnicas que ajudam a atingir os objetivos da segurança da informação, como confiabilidade, confidencialidade, integridade e disponibilidade. O desenvolvimento de ferramentas como criptografias, firewall, senhas e tokens são exemplos de mecanismos de segurança da informação.

Contudo, a busca por um algoritmo que garanta inviolabilidade do sistema criptográfico, associada às constantes mudanças tecnológicas elevou a complexidade da segurança da informação. A difusão das inovações no campo da criptografia permeou praticamente todas as tecnologias de informação e comunicação e consequentemente a maioria dos setores da economia, haja vista, a característica de Tecnologia de Uso Geral[1], (*General Purpose Technology*) que as TICs possuem. Ou

[1] As tecnologias de informação e comunicação têm sido classificadas como Tecnologias de Propósito Geral (TPG). Atualmente computadores e equipamentos relacionados são utilizados em praticamente todos os setores da economia. As TICs apresentam um nível substancial de dinamismo tecnológico, induzindo não apenas à melhora radical na capacidade computacional, mas também à sucessivas ondas de novas tecnologias. Além disso, as TICs facilitam o caminho para as organizações, descentralizações de tomada de decisão, gerenciamento de equipes etc. (BRYNJOLFSSON e HITT, 2000; BRESNAHAN *et al*., 2002). Conforme (Brynjolfsson e Hitt, 2000) essas características apresentam

seja, a aplicação da criptografia e de outros mecanismos de segurança nos sistema, na internet, nas redes complexas das organizações, na computação móvel, na computação em nuvem, o big data, entre outras tecnologias, demonstra a importância que a segurança da informação tem na economia ao reduzir o risco de perda financeira e de reputação que as organizações estão expostas ao atuarem no ambiente digital.

Ao considerar que os problemas que surgem no campo da segurança da informação são limitadores de adoção de novas TICs no setor financeiro, mesmo sendo um setor intensivo no uso de tais tecnologias. Apresenta-se a necessidade de formular estudos que esclareçam como esses problemas têm demandando novas soluções do setor de segurança da informação.

Com o avanço da tecnologia, surgiram novos canais para a oferta de produtos e serviços, como a *internet bank* e *mobile banking*, fontes de oportunidades para o aumento de eficiência e transparência. Em contrapartida, garantir a segurança das informações, diante da necessidade contínua de realizar investimentos em TICs para expandir as operações e fazer frente ao contexto de concorrência, tem sido um desafiador.

De acordo com o comitê gestor de segurança bancária da FEBRABAN – Federação Brasileira de Bancos, (2012), o setor financeiro investe cerca de 40% do recurso anual destinado a TI, aproximadamente R$ 8 bilhões na área de segurança de informação. Os investimentos buscam garantir os quatro objetivos principais da segurança da informação: confiabilidade, confidencialidade, integridade e disponibilidade dos dados do sistema bancário.

Diante do exposto, o presente trabalho busca apresentar a evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro. O trabalho está estruturado em quatro capítulos, sendo o primeiro introdutório, o segundo a apresentação do referencial teórico que resgata importantes elementos da inovação abordados por Shumpeter e Neo-Schumpeterianos, especialmente dos regimes tecnológicos e de trajetórias tecnológicas. O terceiro capítulo destina-se a evolução do setor de segurança da informação segundo a análise dos regimes tecnológicos para o setor. O quarto capítulo apresenta a evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro, onde se estabe-

---

efeitos positivos de aumento da produtividade, especialmente se associados a investimentos em outros ativos intangíveis como P&D, capital organizacional e capital humano.

lece a conexão com a definição de *demand-pull* em Paradigmas Tecnológicos e Trajetórias Tecnológicas de Dosi (1982). Por fim, as considerações finais.

.

2 REFERENCIAL TEÓRICO

2.1 ASPECTOS GERAIS DA INOVAÇÃO

Existe um consenso a respeito da influência que as inovações tecnológicas exercem sobre a estrutura da indústria e sobre a organização das instituições. O entendimento de que a inovação e o desenvolvimento tecnológico são determinantes, tanto no aumento da produtividade, quanto do emprego, fez com que muitos avanços teóricos ocorressem no último século nesta área de conhecimento da ciência econômica.

Quando Schumpeter (1982) formulou sua teoria do desenvolvimento econômico, tratou a inovação como fator de diferenciação competitiva entre as empresas e componente essencial da dinâmica capitalista, e a deixou com o status de elemento central para a explicação de sua abordagem. O autor atribuiu grande importância àquelas inovações tecnológicas radicais responsáveis por significantes transformações, ao ponto de afastar o equilíbrio atual.

Após as contribuições de Schumpeter, surgem então os autores Neo-Schumpeterianos,considerados seus seguidores, e que também observam o progresso tecnológico como principal ator do desenvolvimento econômico. No entato, consideram que as inovações incrementais são elementos que determinam mudanças na dinâmica econômica, devido ao fato que estas ocorrem com uma freqüência maior do que as inovações radicais.

2.1.1 As contribuições da abordagem de Schumpeter para o entendimento da inovação

Schumpeter (1982) faz uma análise da estrutura industrial da europa do início do século XX, onde o desenvolvimento seria caracterizado pela ruptura do fluxo circular do sistema econômico, por meio do surgimento de inovações. Para ele

as inovações representam um elemento determinante do processo de mudança que caracterizam o desenvolvimento do capitalismo. Nessa visão, os empresários são os atores principais na implementação de invenções na área produtiva, assim como na geração e disseminação das inovações, em forma de ondas no sistema econômico. Tornando assim, obsoletas as demais tecnologias existentes no mercado.Este processo de “destruição criadora”, ou seja a substituição de antigos produtos e hábitos de consumir por novos, seria conceito primordial para se entender o capitalismo. É dele que se constitui o capitalismo e a ele deve se adaptar toda a empresa capitalista para sobreviver. (SHUMPETER,1961,p.110)

Nesta visão, o desenvolvimento não ocorre de forma contínua, mas sim alternando períodos de crescimento e de rescessão. Sendo que no caso de crescimento estão associados à difusão de inovações-chave no sistema produtivo. Isso porque o sucesso daquelas empresas inovadoras que buscam lucros monopolistas por meio das inovações, passa a ser imitado por outros empreendedores, gerando assim, uma onda de investimentos, que estimulam a economia (SCHUMPETER, 1982). Acrescenta que em setores com altas barreiras à entrada, as inovações são realizadas, sobretudo, pelas grandes empresas, enfatizando que estas tem o papel de motor do crescimento econômico. Denominando “acumulação criativa” o processo de acumulação de conhecimento não tranferível em mercados tecnológicos, onde a concentração de mercado apresenta-se como fator determinante no surgimento da inovação (SCHUMPETER, 1982).

Para o autor, para que houvesse inovação seria necessária a existência de três elementos: sendo o primeiro a ideia, ou seja, a criação de um bem ou serviço. O segundo elemento a existência do empreendedor, àquele agente disposto a apropriar-se do risco, e o terceiro elemento, o crédito, que é a fonte de alimentação, para que haja a remuneração do capital, o lucro. E os fatores necessários para o desenvolvimento não teriam os mesmos efeitos, pois não deveriam ser apenas analisados de forma cartesiana e matemática, dado que tais fatores ou variáveis não atuam de maneira lógica, mas sim de forma aleatória, e que os componentes do desenvolvimento que são responsáveis pelos saltos que se verificam no sistema econômico, são os mais importantes nessa visão (SCHUMPETER, 1951).

Em um sentido amplo, a inovação é o impulso que mantém a máquina capitalista funcionando. Essas inovações não são apenas aquelas tecnológias que incorrem no surgimento de novos produtos ou novos processos, mas também são consideradas as descobertas de fontes de matérias-primas, de novos mercados ou de novas formas de organização industrial que surgem através das empresas capitalistas (SCHUMPETER, 1982).

A teoria da inovação sob a ótica de Schumpeter afirma que as longas ondas dos ciclos do desenvolvimento no capitalismo resultam da conjugação ou da combinação de inovações, que criam um setor líder na economia, ou um novo paradigma que passa a impulsionar o crescimento rápido dessa economia. Logo, os investimentos nas novas combinações de produtos e processo produtivos de uma empresa repercutem diretamente em seu desempenho financeiro, de modo que, o moderno empresário capitalista deve ocupar ao mesmo tempo um papel de liderança econômica e também tecnológica. Diante desta visão, Schumpeter (1951) caracteriza o processo de produção como uma combinação de forças produtivas que incluem partes materiais e imateriais. No nível material, tem-se que os fatores originais de produção, seriam terra e trabalho de onde procedem todos os bens. As forças imateriais seriam fatos técnicos e de organização social ou meio ambiente sociocultural. Mais especificamente o meio ambiente sociocultural representaria todo o complexo social, cultural e institucional da sociedade do ponto de vista econômico, ou seja, este meio ambiente especifica as regras dos jogos institucionais, que devem ser observadas na alocação e distribuição. Desta maneira, a estrutura desta economia determina se ela é competitiva ou monopolista, capitalista ou socialista.

2.1.2 As contribuições Neo-schumpeterianas para o entendimento da inovação

Os autores neo-schumpeterianos são identificados por dois grupos importantes. Um deles os que buscam uma abordagem evolucionista, onde se destacam Nelson e Winter, e o outro grupo chamado de corrente homogênea onde se destacam: Dosi, Freeman,Pavitt, Soette, Perez entre outros.

Nelson e Winter (1982) abordaram a analogia entre economia e biologia, onde as mudanças econômicas - tanto no aspecto técnico-produtivo que remete à processos e produtos, quanto na estrutura e dinâmica de mercado que remete a concentração, rentabilidade, diversificação e crescimento – tem origem na busca incessante, por parte das empresas, para introduzir inovações, e estas estariam sujeitas aos mecanismos de seleção de concorrência e mercado, tal qual acontece na teoria Darwiniana onde a evolução das espécies acontece por meio das mutações genéticas submetidas à seleção do ambiente.

A teoria evolucionista tem dois pontos principais de destaque que rompem com o modelo neoclássico. Primeiramente o abandono da ideia de que a racionalidade dos agentes econômicos se expressa através de decisões baseadas em maximizazação de lucro. Isso, devido a existência de incerteza, especialmente pela ocorrência de mudanças estruturais, particularmente as tecnológicas, de previsibilidade limitada, fazendo com o que os agentes optem pela rotina na tomada de decisão e no esforço inovador. Outro ponto é que o equilíbrio da visão neoclássica é abandonada em detrimento da noção de desequilíbrio e assimetrias, considerados por Nelson e Winter como fatores essenciais para mudança estrutural e do movimento (POSSAS, 1989).

Ao tratar da questão da hipótese da maximização dos lucros como expressão da racionalidade dos agentes, especialmente da firma, a abordagem evolucionista, direciona a análise para um compotarmento cauteloso do tomador de decisão. Quando a empresa se depara com uma situação de dilema, em que o futuro não se pode prever, o empreendedor adota uma conduta de cautela a partir de procedimentos de rotina, afim de minimizar os efeitos das consequências de tomar decisão sem que haja segurança quanto aos resultados. Esse comportamemento conservador, devido ao ambiente incerto, é melhor expresso pela emprego de rotinas no processo de decisão. Uma vez que os resultados das decisões de investimentos, particularmente em inovações, possuem uma natureza irrevogável, deve haver alguma norma habitual, convencional ou rotineira para tomada de decisão, que revelam menor risco (POSSAS, 1989).

Segundo Nelson e Winter (1977) a adoção de rotinas serve para minimizar o risco do tomador de decisão que se vê em um ambiente com pouca previsibilidade.

Sendo o emprego desta, a rotina, uma medida cautelosa que procura evitar custos de uma decisão equivocada por falta de previsibilidade dos fatores.

Em sua primeira publicação, Winter definiu a rotina como “padrão de comportamento que é seguido repetidamente, mas estão sujeitas a mudanças, caso as condições se alterem” (WINTER, 1964, p.263). Mais tarde explicou que o emprego desse termo serve para incluir características da firma como rotinas técnicas bem especificadas para produzir bens, por meio de procedimentos, intensificação da produção de itens de alta demanda, política de investimento, pesquisa e desenvolvimento, estratégias de diversificação de produtos (NELSON e WINTER, 1982). Os autores traçam paralelos entre rotinas organizacionais e genes, entre empresas e organismos e entre setores e as espécies. Sendo que o resultado do processo de seleção econômica é a sobrevivência das empresas dentro de um setor (NELSON E WINTER, 1982).

Ou seja, se o comportamento das empresas na tomada de decisões é governado por procedimentos de rotinas, não significa que os resultados também sejam rotineiros, pois tanto regras simples, como regras estocásticas determinam as mudanças de comportamento. Além de serem caracterizadas pela repetição, as rotinas também são caracterizadas pela experimentação, o que sugere ganho de tempo e qualidade e consequente surgimento de oportunidades (CORAZZA E FRANCALANZA, 2004).

Nelson e Winter (1982) reconhecem as diferenças entre a rotinas mais simples como gerenciamento de pedidos ou de estoques e outras rotinas que envolvem maior análise como a decisão da proporção ideal de publicidade em relação as vendas ou então a decisão da construção de uma nova planta. Entretanto, para a teoria evolucionária, a rotina é tratada como uma unidade de análise*, que servem para* entender melhor as mudanças na economia (BECKER, 2006).

2.2 REGIMES TECNOLÓGICOS

De acordo com Malerba (2007) regimes tecnológicos são definidos pela combinação de oportunidades tecnológicas, apropriabilidade das inovações, cumulatividade dos avanços técnicos e as propriedades da base de conhecimentos presentes em atividades inovadoras das empresas. A noção de regime tecnológico proporciona uma forma sintética de representar algumas das propriedades econômicas mais importantes das tecnologias e das características dos processos de aprendizagem envolvidos em atividades inovadoras. Tornando possível identificar algumas condições estruturais fundamentais que definem as competências necessárias, os incentivos e as propriedades dinâmicas do processo inovativo.

A noção de regimes tecnológicos foi apresentada por Nelson e Winter (1982). Os autores descreveram o ambiente inovativo que as empresas operam e interpretaram os processos inovativos. Definindo dois tipos de regimes tecnológicos, um de base cumulativa, em que a inovação ocorre de forma incremental e por isso as oportunidades tecnológicas são mais difíceis de serem exploradas. E outro, de base científica, em queonde as oportunidades são mais numerosas e de mais fácil acesso.

Em outros trabalhos, Nelson e Winter (1982) e Winter (1984) descrevem esses diferentes regimes tecnológicos básicos, a partir da característica da base de conhecimento: sendo um, o regime empreendedor, em que a base de conhecimento está relacionado com a ciência e não cumulativo e universal (facilitando assim a entrada de novos empresas), e outro, o regime rotinizado que é mais cumulativo e interno a indústria (facilitando assim a inovação por empresas estabelecidas).

De acordo com Marlerba (2007) tanto a estrutura, como a organização de atividades inovadoras apresentam características diferentes entre os setores da economia. Sendo que em determinados setores, as atividades inovadoras estão concentradas entre poucas empresas, enquanto que em outros setores, as atividades inovadoras são distribuídas entre várias empresas. Desse modo, a diferença entre estas atividades inovativas pode ser atribuída aos padrões principais de inovação identificados por Schumpeter e que ficaram conhecidos na literatura como Schumpeter Mark I e Schumpeter Mark II.

Em Schumpeter (1911), Mark I, “A teoria do desenvolvimento econômico”, o padrão é caracterizado pela “destruição criadora”. Devido a facilidade de entrada, ao papel principal desempenhado por empresários e por novas empresas em atividades inovativas, que desafiam as firmas estabelecidas e as atuais formas de produção, organização e distribuição, destruindo completamente as quase rendas associadas com inovações prévias. Já em Schumpeter (1942), Mark II, em “Capitalismo, socialismo e democracia”, o padrão da atividade inovativa é caracterizado por “acumulação criadora” com a presença de grandes firmas estabelecidas e de barreiras à entrada de novos inovadores. A partir do estoque de conhecimento acumulado em áreas tecnológicas específicas, competências em P&D, produção e distribuição e recursos financeiros relevantes, formam-se barreiras relevantes a entrada de novos empreendimentos e pequenas empresas.

Outros autores depois de Nelson e Winter, como Gort e Klepper (1982), Cohen e Levin (1989) e Audretsch (1997), entre outros, tem relacionado que mais do que o tamanho da empresa ou da demanda, a oportunidade e as condições de apropriabilidade aparecem como os mais relevantes fatores que afetam a dinâmica da estrutura de mercado e inovação.

As características do processo de aprendizado envolvido nas atividades inovativas e juntamente com as propriedades econômicas das tecnologias destas atividades foram sintetizadas nesta noção de regime tecnológico.

Ao introduzir a noção de regime tecnológico, Nelson e Winter (1982) descreveram o ambiente tecnológico em que as empresas atuam, e explicaram os diversos processos inovativos observados entre setores industriais, classificando estes setores em poucas categorias com características comuns. Construíram modelos de simulação para demonstrar que o ambiente tecnológico, em termos de condições de oportunidade e apropriabilidade, alteram a intensidade da inovação, o grau de concentração industrial e a taxa de entrada em uma indústria. Dessa forma, as oportunidades tecnológicas, no regime de base científica, são mais numerosas e podem ser acessadas com maior facilidade. Enquanto que as oportunidades tecnológicas são mais difíceis de serem exploradas no regime de tecnologia cumulativa, pois a inovação ocorre de forma incremental.

Malerba e Orsenigo (1990, 1993); Breschi, Malerba e Orsenigo (2000); Malerba (2007), definiram o regime tecnológico como uma combinação específica de pro-

priedades fundamentais das tecnologias: condições de oportunidade, apropriabilidade das inovações, graus de cumulatividade do conhecimento dos avanços técnicos e características da base de conhecimento relevante, conforme apresentados a seguir.

Oportunidades tecnológicas refletem a probabilidade de inovar para qualquer quantidade dada de dinheiro investido em pesquisa. Elevadas oportunidades fornecem incentivos para a realização de atividades inovadoras e denotam um ambiente econômico que não é limitado pela escassez. Onde quatro dimensões básicas de oportunidade podem ser identificados: nível, variedade, capilaridade[2] e fontes.

Nível: O nível de oportunidades determina a probabilidade de inovar para uma determinada quantidade de recursos investidos em P&D. Assim, elevados níveis de oportunidades provêem incentivos para as atividades inovativas.

Variedade: A variedade de soluções tecnológicas pode estar associada à elevados níveis de oportunidades. A alta variedade de soluções tecnológicas sugere que o conhecimento pode ser aplicado a uma ampla gama de produtos e mercados.

Capilaridade: A capilaridade de oportunidades refere-se à aplicabilidade dos novos conhecimentos em outros produtos e mercados. A alta capilaridade de oportunidades revela que novos conhecimentos podem ser aplicados em vários produtos e mercados. Enquanto que no caso de baixa capilaridade de oportunidades faz com que novos conhecimentos apenas sejam aplicados em poucos produtos e mercados.

Fontes: As fontes de oportunidades tecnológicas referem-se à sua origem. Podendo ser relacionados aos avanços científicos em universidades, avanços em P&D, aprendizado endógeno, aprendizado a partir de fornecedores ou clientes (FREEMAN,1982;ROSENBERG,1982 e NELSON,1993).

A base de conhecimento indica as propriedades do conhecimento em que as atividades inovativas se baseiam. Onde Malerba (2007) descreve duas características principais a cerca da base de conhecimento: a natureza do conhecimento e os meios de transmissão.

Natureza do conhecimento: o conhecimento tecnológico envolve vários graus de especificidade, “tacitividade”, complexidade e independência (Winter, 1987). Sendo que algumas dessas características podem mudar durante a evolução de um setor ou tecnologia específica, atingindo maior ou menor grau.

[2] O texto original de Malerba (2007) apresenta o termo *Pervasiveness*.

Meios de transmissão de conhecimento: Os meios de transmissão do conhecimento podem ser formais ou informais. Assim, quanto mais o conhecimento é específico, tácito, complexo e sistêmico, mais relevantes são os meios informais de transmissão, como ensino pessoal e treinamento ou migração de pessoal qualificado. E quanto mais o conhecimento é padronizado, codificado, simples e independente, mais relevantes são os meios formais, como publicações especializadas, licenças e patentes (BRESCHI e MALERBA, 1997).

A cumulatividade dos avanços técnicos indica que a partir do conhecimento e das atividades inovativas realizadas no presente são formadas as bases para o surgimento de inovações no futuro. Ou seja, uma inovação gera um fluxo de inovações posteriores, produzindo melhoria gradual ou original, criando novos conhecimentos que serão utilizados em outras inovações em outras áreas. Assim, elevados níveis de cumulatividade são facilmente reconhecidos em ambientes econômicos que apresentam continuidade em atividades inovadoras e que alcançam retornos crescentes dessas atividades. Como consequência, as empresas inovadoras no presente possuem maiores chances de inovar no futuro, quando comparadas com empresas que não inovam (MALERBA E ORSENIGO, 1997 e MALERBA, 2007).

Em Malerba (2007), processos de aprendizado, fontes organizacionais e sucesso anterior foram identificados como fontes de cumulatividade, conforme descritas a seguir:

Processo de Aprendizado: o processo de aprendizado refere-se a geração do novo conhecimento a partir do conhecimento adquirido em atividades anteriores. Onde, a natureza cognitiva dos processos de aprendizagem e conhecimento passado delimitam a pesquisa atual, podendo gerar novas questões e novos conhecimentos.

Fontes Organizacionais: indicam a origem da cumulatividade. Podendo ser do estabelecimento de instalações de P&D, capaz de produzir um fluxo estável de inovações. De modo geral, podem ser originadas de capacidades específicas das empresas, podendo ser melhoradas gradualmente ao longo do tempo, definindo o que a empresa pode fazer agora e o que pode buscar alcançar no futuro.

Sucesso Anterior: refere-se à cumulatividade obtida a partir do resultado alcançado com a atividade inovativa anterior. Schumpeter (1942) relaciona os feedbacks críticos do mercado com investimento em P&D, o desempenho tecnológico e

rentabilidade. Outro argumento para explicar esta fonte está em Nelson e Winter (1982), onde os autores sugerem que a persistência pode ser simplesmente o resultado do sucesso anterior, conhecido originalmente como *success-breeds-success* (em português: sucesso gera sucesso). Ou seja, o sucesso inovador rende lucros que podem ser reinvestidos em P&D, aumentando assim, a probabilidade de inovar novamente.

A apropriabilidade das inovações resume as possibilidades de proteger as inovações de imitações e de colher os lucros dessas atividades inovadoras. Sendo duas as dimensões básicas: o nível e os meios de apropriação.

Nível: refere-se às condições de alta ou baixa apropriabilidade (Levin *et. al*, 1987). Se a condição for de alta apropriabilidade significa que existem formas seguras de proteger a inovação de imitações. Se a condição for de baixa apropriabilidade, significa então, que o ambiente é caracterizado pela rápida transferência de conhecimento.

Meios de Apropriação: Trata-se de mecanismos utilizados para proteger as inovações. Estes diferem entre as indústrias, assumindo diferentes formas, como patentes, inovações contínuas e controle de ativos complementares (TEECE, 1986; LEVIN ET AL. 1987).

2.3 PARADIGMAS TECNOLÓGICOS E TRAJETÓRIAS TECNOLÓGICAS

Giovanni Dosi (1982) buscou identificar o que causa o progresso tecnológico e como o progresso ocorre a partir da formulação de um marco teórico que explica a natureza do processo de mudança tecnológica.

Segundo a concepção de Dosi (1982) a tecnologia é um conjunto de conhecimento, prático ou teórico, mesmo que ainda não aplicados, incorporado à atividade econômica e que combina objetivo de sobrevivência no mercado através de novos processos e novos produtos. Envolvendo procedimentos, métodos, experiências, know-how, mecanismos e equipamentos, arranjos institucionais, entre outros. Segundo o autor, a tecnologia demonstra um caráter dinâmico e endógeno ao processo

de desenvolvimento econômico, diferentemente do conceito estático da teoria neoclássica.

O paradigma tecnológico, por sua vez é definido como um “modelo” ou um “padrão” de soluções de um conjunto de problemas de ordem técnica, selecionado a partir de princípios derivados do conhecimento científico e das práticas produtivas. Significa que a busca da solução de determinados problemas tecnológicos concentram-se naquelas soluções já conhecidas, juntamente com os esforços para aperfeiçoar a base de conhecimento (DOSI, 1982). Em Dosi (2006), tem-se o paradigma tecnológico como um pacote de procedimentos que orientam uma determinada investigação sobre um problema tecnológico, definindo assim, o contexto e os objetivos a serem alcançados e também os recursos a serem utilizados.

De acordo com (Cimoli e Dosi, 1994b) a noção de paradigma tecnológico se baseia em uma visão sobre tecnologia consolidada em três fundamentos: primeiramente, a definição de tecnologia deve satisfazer a representação da forma específica do conhecimento e como estão baseadas estas atividades. Sendo esses voltados para solucionar problemas envolvidos, sejam eles, individuais e ou organizacionais. Em segundo lugar, os paradigmas implicam heurísticas e conceitos específicos de "como fazer as coisas" e como melhorá-las, o que, geralmente, é comum em várias atividades profissionais (engenheiros, empresas, sociedades técnicas). Por fim, esses paradigmas também definem normalmente os modelos básicos de produtos industriais e sistemas de produção que são progressivamente modificados e melhorados. Essas *commodities* também podem ser descritas com base em algumas características fundamentais de caráter tecnológico e econômico.

Dosi (1984) define duas teorias determinantes para o paradigma da inovação tecnológica.

Primeiramente, define a teoria de *demand pull*, onde as forças do mercado são os principais determinantes para a mudança técnica, e as inovações tecnológicas são determinadas de forma reativas, ou seja, as inovações ocorrem frente às necessidades geradas pelo mercado, conforme segue:

a) Existe um conjunto de bens de consumo e bens intermediários, num determinado momento, no mercado, satisfazendo diferentes necessidades por parte dos compradores;

b) Os consumidores expressam suas preferências sobre as características dos bens que desejam através de seus padrões de demanda;

c) A restrição de renda marginal leva ao aumento das opções (devido à preferência do valor pessoal);

d) Produtores percebem as necessidades reveladas pelos consumidores e usuários: algumas dimensões de utilidade possuem maior peso; e,

e) Início do processo de inovação: as empresas bem-sucedidas terão que apresentar bens novos ou melhorados para o mercado e o círculo começa outra vez desde o início.

A outra teoria apresentada por Dosi (1984) é a *technology-push*, em que a inovação tecnológica age de maneira autônoma ou semi autônoma, e que num segundo momento irá impactar na econômica, onde destacam:

a)O papel crescente dos insumos científicos no processo inovador;

b) O aumento da complexidade de P&D que torna o processo inovador de uma questão de planejamento de longo prazo para a empresa;

c) Uma correlação significativa entre esforços em P&D e difusão de inovação em diversos setores industriais;

d) A natureza intrinsecamente incerta da atividade inventiva, que joga contra uma hipótese de conjuntos limitados e conhecidos de escolhas e resultados.

A trajetória tecnológica é definida como o resultado do modo ou padrão das formulações e soluções de problemas específicos dentro do paradigma (DOSI, 1982). Segundo (Cimoli e Dosi, 1994b) o conceito de trajetórias tecnológicas está associado ao desenvolvimento progressivo de oportunidades de inovação em cada paradigma. Podendo ser medidos pelas alterações das características técnico-econômicas de produtos e processos. Assim, as noções fundamentais desse conceito são dadas por cada conjunto específico de conhecimento, dando forma, restringindo e direcionando as mudanças tecnológicas, havendo ou não estímulos no mercado. E consequentemente, pela regularidade dos padrões de mudanças técnicas em diversas condições de mercado, onde a interrupção se dá pela mudança radical na base de conhecimento.

Uma importante referência na definição da trajetória é certamente da contribuição de Kuhn (2003), com distinção entre ciência normal e mudança paradigmática. As trajetórias então aparecem como uma tradução e aplicação da noção de ciên-

cia normal que se move sobre uma predeterminada rota até a sua habilidade heurística de se esgotar. Nessas circunstâncias, existem condições para uma definição de continuidade, ou seja, a ocorrência de mudança paradigmática (Antonelli, 2003, p21).

Giovanni Dosi (1982) elenca seis principais características que auxiliam no entendimento das trajetórias tecnológicas, conforme a seguir:

a) Pode haver várias trajetórias, que podem ser mais fortes que outras, bem como a variação de costumes;

b) Há complementaridades entre as trajetórias, bem como a evolução de outras tecnologias;

c) Um modelo pode definir a fronteira tecnológica em relação ao caminho por ele percorrido ante as dimensões econômicas; ou o modelo científico pode estabelecer uma relação econômica;

d) O progresso de uma trajetória tende a reciclar algumas características cumulativas;

e) Especialmente quando há uma trajetória é dominante, pode ser difícil de mudar o caminho, para um caminho alternativo, dificultando assim, a comparabilidade entre os dois;

f) É duvidoso se é possível a priori, comparar, avaliar a superioridade de uma trajetória tecnológica em detrimento de outra.

Há efetivamente alguns critérios a serem escolhidos, alguns indicadores. Esta é uma das razões por trás da natureza íntima e incerta da atividade de pesquisa (mesmo deixando de lado as avaliações de mercado dos resultados, mas apenas considerando indicadores puramente tecnológicos).

A noção de trajetória tecnológica baseia-se nas realizações obtidas com o ciclo de vida do produto e torna possível a existência de uma fonte da pesquisa cumulativa na disciplina (ANTONELLI, 2003, p21). Rosenberg (1982) contribuiu na análise de mudanças técnicas com a noção de convergência tecnológica que salienta a dinâmica de misturas de tecnologias em suas relações. A introdução de tecnologias-chave pode ativar uma gama de inovações derivadas, fundamentadas em uma mudança tecnológica incremental (ROSENBERG 1976; 1982).

Segundo Dosi (1982), as mudanças contínuas são frequentemente relacionadas com o progresso no decorrer de uma trajetória tecnológica definida por

um paradigma tecnológico. Enquanto que as mudanças descontínuas são associadas com o surgimento de novos paradigmas. A origem dos paradigmas tecnológicos deriva da interação do avanço científico, fatores econômicos, variáveis institucionais e dificuldades não solucionadas em um caminho tecnológico estabelecido. Assim, a função da tecnologia e da inovação tecnológica é muito mais ampla, ou seja, são partes que completam o todo, ou compõe o conhecimento, que tem em partes funções práticas, relacionadas a problemas, como também à teoria, e a união da teoria com a prática resulta na formação de Know-how, métodos, teste empíricos que podem resultar em sucessos ou fracassos.

3 EVOLUÇÃO DA SEGURANÇA DA INFORMAÇÃO

A primeira seção deste capítulo compreende uma breve apresentação das definições da segurança da informação da literatura atual. A segunda seção é dedicada à apresentação da origem da segurança da informação até o estado atual do desenvolvimento das ferramentas que asseguram a segurança da informação das organizações. A terceira seção busca discutir a evolução do setor de segurança da informação segundo os regimes tecnológicos e caracterizar o setor de segurança da informação como um setor orientado pelas demandas de mercado (*demand- pull*).

3.1 DEFINIÇÃO DA SEGURANÇA DA INFORMAÇÃO

A relevância da informação para as organizações tem crescido a cada dia. A informação nos dias de hoje é um ativo, que é mensurável e logo pode ser negociada. Portanto o conceito de segurança da informação ganhou importância na sociedade, pois está diretamente associada às medidas de proteção e prevenção, contra ameaça de roubo, adulteração, destruição, acesso, uso indevido e indisponibilidade da informação (LORENS, 2007).

Segundo a NBR ISO/IEC 17799:2000 (código de prática para a gestão da segurança da informação), a informação é um ativo importante para os negócios como qualquer outro e devido ao seu valor deve ser adequadamente protegida. Portanto a segurança da informação protege a informação de diversos tipos de ameaças, a fim de garantir a continuidade dos negócios, minimizando danos e maximizando o retorno dos investimentos, bem como as oportunidades de negócio (ABNT, 2000).

Sêmola (2003) conceitua segurança da informação como uma área de conhecimento dedicada à proteção de ativos de informação, contra acessos não autorizados, contra alterações indevidas e contra a indisponibilidade. Não contemplando em sua visão as relações sociais envolvida nos fenômenos informacionais.

Pode-se dizer que, como disciplina, a segurança da informação ainda está em fase de consolidação. Uma vez que geralmente é associada a um conjunto de técnicas ligadas a suportes tecnológicos. Como a literatura tem abordado a segurança da informação muito mais pelo aspecto funcional, esta visão tem dificultado o surgimento de uma concepção mais holística, mais social, mais fenomenológica e faz com que os aspectos humanos sejam pouco discutidos. Hitchings (1994) e Anderson (2003), em seus respectivos trabalhos, abordam essa questão e sugerem definições para a Segurança da Informação.

Hitchings (1994) sugeriu a importância de considerar as questões humanas na concepção de segurança da informação e usa uma 'metodologia virtual' para considerar controles humanos centrado em uma organização e seu ambiente. Claramente uma falta de controle da atividade humana pode resultar no aumento da ocorrência de incidentes. Como exemplos, empregados descontentes, oportunidades a serem exploradas e até mesmo, um gestão inadequada também pode ser considerado como precursores de um ambiente antiético. Tornando assim, a organização, em questão, vulnerável a crimes.

Anderson (2003) em seu artigo "*Why we need a new definition of information security*" sugere que o equilíbrio entre riscos e controles, percebidos através de uma convicção bem fundamentada de segurança, que é subjetiva, é uma definição razoável para a segurança da informação, pois introduz o fator humano na definição da segurança da informação.

Summers (1997) define a Segurança da Informação como uma meta a ser atingida de proteger os sistemas de computadores de ameaças à confidencialidade, integridade e disponibilidade.

A norma ISO/IEC 27002:2005, em sua seção introdutória, define segurança da informação como a proteção da informação de diversos tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Protegendo a informação das ameaças à sua integridade, disponibilidade e confidencialidade, a fim de garantir a continuidade do negócio e minimizar os riscos. A norma ISO/IEC 27000:2009 mantém a definição de 2005, e acrescenta propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade (LORENS, 2007).

Contudo, as definições agregam conceitos que refletem a evolução da segurança da informação frente ao avanço das tecnologias, da forma como ocorrem os incidentes e como surgem as ameaças às organizações.

3.2 A ORIGEM DA SEGURANÇA DA INFORMAÇÃO

Existem inúmeras evidências na história de que o ser humano busca guardar segredos. Sejam esses segredos militares, industriais, governamentais, familiares, ou religiosos, a busca por manter algo em sigilo, traz em sua causa raiz interesses e princípios, que variam de acordo com a cultura de um povo, com suas crenças e, sobretudo com o tempo. Entretanto, assim como evoluíram os métodos para manter segredos, a busca por desvendar segredos apresenta-se em diversos contextos, mas especialmente os que envolvem disputas poder econômico.

Para apresentar a origem da segurança da informação, é necessário recorrer à trajetória da criptografia ao longo do tempo. De acordo com Kahn (1967, p.64-67), cerca de 4.000 anos atrás os egípcios deixaram marcas de elementos essenciais da criptografia, a partir de transformação da escrita comum. As inscrições do túmulo de Khnumhotep II (um arquiteto do faraó Amenemhet II) demonstram evidências da utilização de símbolos hieróglifos incomuns no lugar outros comuns. Mais tarde, cerca de 1.500 A.C., os mesopotâmicos registraram o uso da criptografia numa fórmula para fazer esmaltes para cerâmica. A partir do uso de símbolos especiais com significados diversos. Nesta época, os assírios usaram intáglios, peças planas de pedra com símbolos entalhados para a sua identificação.

Outro importante período a destacar como um salto na criptologia, ciência que estuda a criptografia, é o do império romano, cerca de 50 A.C.. Quando o imperador romano Júlio César, utilizou-se da cifra por substituição, para cifrar mensagens governamentais. O criptograma de César, usado pelos imperadores romanos para enviar mensagens aos generais consistia no uso de uma tabela de referencia ao alfabeto a partir de uma regra pule três. As letras deveriam ser substituídas pela terceira letra seguinte do alfabeto (KAHN, 1967, p.64-67). Como exemplo a cifragem da famosa citação de César, "veni, vidi, vici" (tradução: Eu vim, eu vi, eu conquistei)

com uma mudança cesariana de três, se traduziria em "YHQL YLGL YLFL". A técnica foi muito utilizada, porém com o tempo o segredo foi descoberto, surgindo assim, a necessidade de desenvolver novos métodos (BUTACCIO, 2003).

Em meados do século XVI, os estudos de Blaise de Vigenère desenvolveram uma nova cifra que também utilizava substituição de letras assim como as de César, entretanto funcionava com uma tabela de referência maior e eram cifradas de maneira diferente, o que tornava inviável a análise de freqüência de ocorrência das letras, e dificultava a criptoanálise. O método ficou conhecido como o de substituição polialfabética, uma generalização do método mono alfabético de César (KAHN, 1967, p.64-67).

Esses métodos foram eficientes até o final do século XIX e início do século XX. Tornaram-se obsoletos devido ao surgimento de máquinas com princípios mecânicos e elétricos. Primeiro surgiu o engenhoso cilindro de madeira de Thomas Jefferson[3]. Um tubo de 15 cm, com discos que continham o as letras do alfabeto gravadas e randomicamente organizadas em suas extremidades. A partir de uma mensagem, as rodelas eram embaralhadas e apenas aqueles que possuíssem a combinação exata do posicionamento das rodelas poderia então ler a mensagem original. Depois, durante a Segunda Guerra Mundial, com a criação de uma máquina nazista batizada de Enigma, usada para camuflar as estratégias militares, a máquina propunha novo sistema de criptografia, com princípios que mais se assemelham aos utilizados nos tempos atuais (BUTACCIO, 2003).

As décadas de 1950 e 1960 representam os primeiros passos para a segurança da informação na era dos computadores. A principal preocupação dessa área estava no campo da confiabilidade dos computadores e no controle de acesso físico aos equipamentos. Nesse período havia poucos computadores e especialistas em linguagem de programação. Conforme Cherdantseva e Hilton, (2012) nesse período não há relatos de violação.

Até o final dos anos 1950 apenas as agências do governo possuíam computadores. E a grande mudança acontece apenas em 1964 quando a IBM lançou o mainframe com a versão chamada de IBM System/360, que se destacavam pela alta

[3] Ainda secretário de estado de George Washington, Thomas Jefferson, mais tarde se tornaria presidente dos Estados Unidos. Jefferson confiava cartas importantes a mensageiros que as entregavam pessoalmente, porém quando se tornou ministro americano para a França, os códigos foram de suma importância para evitar que agentes do correio europeu lessem as suas mensagens) (Buttaccio, 2003).

capacidade desempenho de processamento. O equipamento foi vendido em larga escala para grandes corporações especialmente para instituições financeiras (SINGH, 2001). Desde então a companhia, que detinha cerca de 70% do mercado de mainframes e tornou-se referência para esse modelo de computadores. (TIGRE, 1984).

Nesse período, os mainframes eram sinônimos de segurança da informação. Chamados no mercado de RAS, (Reliability, Availability, Serviceability), que significa Confiabilidade, Disponibilidade, Facilidade de Manutenção, eram conhecidos como equipamentos seguros e acessíveis a múltiplos usuários (PHILIPSON, 2002).

Durante a década de 1960, devido o crescente uso dos computadores surgiu a necessidade de obter privacidade e proteger a informação em formato digital. No entanto, até o início dos anos 1970 as técnicas de criptografia estavam apenas a serviço das agências de segurança, como a NSA (*National Security Agency*).

O fato de que os mainframes eram acessíveis por múltiplos usuários e compartilhado por vários departamentos das organizações deu início as preocupações com o risco de vazamento de informações ou de ataques internos, causados, até mesmo, por um funcionário mal intencionado. Com isso os computadores eram alocados em salas isoladas ou até mesmo em prédios exclusivos, denominados CPDs (Centro de Processamento de dados), onde apenas pessoas autorizadas tinham acesso (MACEDO, 2012).

A chegada dos minicomputadores[4] e posteriormente dos microcomputadores mercado no final dos anos 1970 marca uma mudança importante no setor de segurança da informação. E as questões de integridade e disponibilidade começaram a adquirir maior importância entre os objetivos desse setor. O desenvolvimento de novos softwares foi acompanhado pela chegada dos primeiros vírus de computadores, que no início representava apenas um “troféu” para os programadores, uma demonstração de capacidade de invadir outro ambiente, mas logo passou a chamar a

[4] A inserção comercial dos minicomputadores pela empresa *DEC - Digital Equipament Corporation*. Estes computadores que já existiam há quase 20 anos ganharam o mercado representaram o surgimento de uma nova classe de equipamentos (AUERBACH INFO, 1971). Eram menores, mais baratos que os mainframes, porém com menor capacidade de processamento e de memória. Devido sua característica de adaptação às tarefas relacionadas ao controle de processos e de comunicação. Essa classe de computadores foi importante para o aumento substancial das inovações em software até meados de 1985 quando a sua fabricação entrou em declínio (BELL,2013).

atenção, devido aos primeiros casos de vazamento de informação e prejuízo financeiro (SALTZER e SCHROEDER, 1975).

Diante disso, a criptografia em formato digital passou a ganhar mais importância. Assim, em 1975, com a apresentação da cifra *DES* (*Data Encryption Standard*) definiu-se nos EUA o início de uma nova fase para a criptografia. Tratava-se de um algoritmo de chaves secretas desenvolvido por um grupo de pesquisadores da IBM em conjunto com o *NIST* (*National Institute of Standards and Technology).* O algoritmo representou para o setor privado, especialmente o setor financeiro um significativo salto do escopo tecnológico disponível para defender as comunicações eletrônicas até o anos 2001 quando foi substituído pelo padrão AES (Advanced Encryption Standard), um método mais seguro e complexo de cifragem que seu precursor. Desenvolvido por belgas, Vicent Rijmen e Joan Daemen, foi o algoritmo vencedor entre outros 15 modelos candidatos em um concurso lançado pelo NIST para definir o padrão que substituiria o DES. O AES também foi considerado mais eficiente pelas características de exigir menos memória dos computadores e também por ser capaz de operar em outros ambientes como de PDAs e *Smart Cards*.

Dieff e Hellman (1976) em *New directions of cryptography* introduziram um novo conceito de cifragem chamado de chave pública. Também chamada de criptografia assimétrica, é baseada no uso de pares de chaves para cifrar e decifrar mensagens. Onde duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais para a codificação da informação. Isso quer dizer que uma chave, chamada chave pública, é utilizada para cifrar, enquanto a outra chave, secreta, é usada para decifrar.

Com a chegada dos microprocessadores 8080 da Intel em 1976, o mercado rapidamente desenvolveu os primeiros microcomputadores que foram vendidos inicialmente pela empresa Apple. Com custo muito mais baixo que os minicomputadores, os microcomputadores, chamados então de PC – Personal Computer, se destacaram pela capacidade de seu processador adaptar-se à hardwares e softwares de diferentes fabricantes (TIGRE e NORONHA, 2013). O PC aos poucos se tornou uma ferramenta comum e acessível, poderosa e fácil de usar. Resultando na propagação do equipamento em lares ou escritórios de pessoas com boas e más intenções

Em 1977, dois pesquisadores do MIT (*Massachusset Institute of Technlogy*), Ron Rivest, Adi Shamir Leonard Adleman, trouxeram o conceito desenvolvido por Dieff e Hellman à realidade. Fundadores da empresa RSA Data Security, Inc., mais tarde incorporada pela EMC Corporation, desenvolveram um algoritmo que considera uma chave pública e outra privada, porém com maior rapidez de processamento e maior segurança do que os seus precursores.

Até os anos 1980 as agências militares eram os principais patrocinadores das pesquisas que movimentavam essa indústria. Entretanto com a proliferação do uso dos computadores no setor comercial, as diferenças de escopo tornaram-se evidentes em relação aos objetivos militares. Dentre outros[5] exemplos, o custo de proteção da informação no mundo corporativo deveria estar equilibrado com o risco para os negócios, diferente dos projetos caríssimos bancados pelo governo norte americano para o desenvolvimento de pesquisas na área (CHERDANTSOVA e HILTON, 2013).

A década de 1980 representa o período onde as oportunidades de inovar no setor de segurança da informação começam a surgir de forma mais intensa. Devido a propagação dos microcomputadores e do desenvolvimento das redes, que aumentou consideravelmente o desafio de TI de proteger o processamento de dados. Conforme Peltier (2009) tratava-se de uma fase de descentralização do processamento de dados, que antes era realizado apenas pelos mainframes nos data centers (CPDs). Mas também, retrata a disseminação de algumas técnicas de gerenciamento de acesso e identificação para outros setores da economia como no industrial, energético, transportes e financeiro.

Nos 1990, com a introdução da internet no meio comercial, a segurança da informação iniciou um importante processo de transformação. A internet levou a criação do comercio eletrônico, aumentou de forma significativa a velocidade com que a informação é transmitida e consequentemente a complexidade dos objetivos de TI em relação à década anterior.

[5]A) O setor de defesa espera um bem financiado, pois o inimigo pode ser forte tecnicamente. No ambiente comercial uma ameaça muitas vezes vem de um funcionário desatento. B) O ambiente de defesa pressupõe pessoa que trabalham em um ambiente protegido fisicamente sob a disciplina militar. O mundo corporativo raramente opera em um ambiente protegido fisicamente; A equipe não é necessariamente de confiança e age nos termos da lei civil. C) A motivação do sector da defesa é baseada na lei, ordens e regulamentos. Os motivos do mundo corporativo são os custos e benefícios (CHERDANTSOVA e HILTON, 2013).

E como resultado do acúmulo de conhecimento desenvolvido tanto em universidades, como em empresas, em 1996 a empresa Netscape lançou o protocolo SSL (*Secure Sockets Layer*). Desenvolvido sobre a plataforma do modelo RSA de criptografia, o modelo confere a segurança da comunicação na internet para serviços como email (SMTP) e navegação por páginas (HTTP). Através da emissão de um certificado eletrônico, que autentica a identidade do servidor, o protocolo é usado para verificação por parte do usuário antes de iniciar uma comunicação, a fim de garantir a utilização do servidor correto. Além disso, impede a interceptação de dados ou vazamentos a partir da criptografia (THOMAS, 2000).

O primeiro caso de invasão à rede de computadores que ganhou notoriedade no mundo corporativo ocorreu nos EUA em 1995. De acordo com New York Times (1995), o russo Vladmir Levin, 34 anos, através de códigos de acessos e senhas de clientes, acessou contas empresariais do banco comercial Citybank, e remeteu cerca de US$ 2,8 milhões para contas em outros bancos.

Desta forma, a partir deste e de outros casos de invasão e ataques articulados sob novas plataformas tecnológicas, o universo de desafios e oportunidades para o campo de segurança da informação se ampliou. Tornando-se indispensável para o modelo atual do setor de TIC e de outros setores da economia.

3.3 A EVOLUÇÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO OS REGIMES TECNOLÓGICOS

De acordo com abordagem teórica dos regimes tecnológicos apresentada no capítulo 1 deste trabalho, os regimes tecnológicos do setor de segurança da informação devem ser definidos a partir da combinação específica de algumas propriedades fundamentais das tecnologias: condições de oportunidade; características da base de conhecimento relevante; graus de cumulatividade do conhecimento dos avanços técnicos; e apropriabilidade das inovações.

3.3.1 Condições de oportunidade

As condições de oportunidade do setor de segurança da informação são observadas a partir da probabilidade da ocorrência de inovação, para determinado nível de investimento em pesquisa. Seguindo os parâmetros definidos por Malerba (2007), a análise desta propriedade deve ser realizada a partir da identificação das quatro dimensões a seguir: a) nível de oportunidade, b) variedade, c) difusão e c)fontes, conforme análise detalhada a seguir.

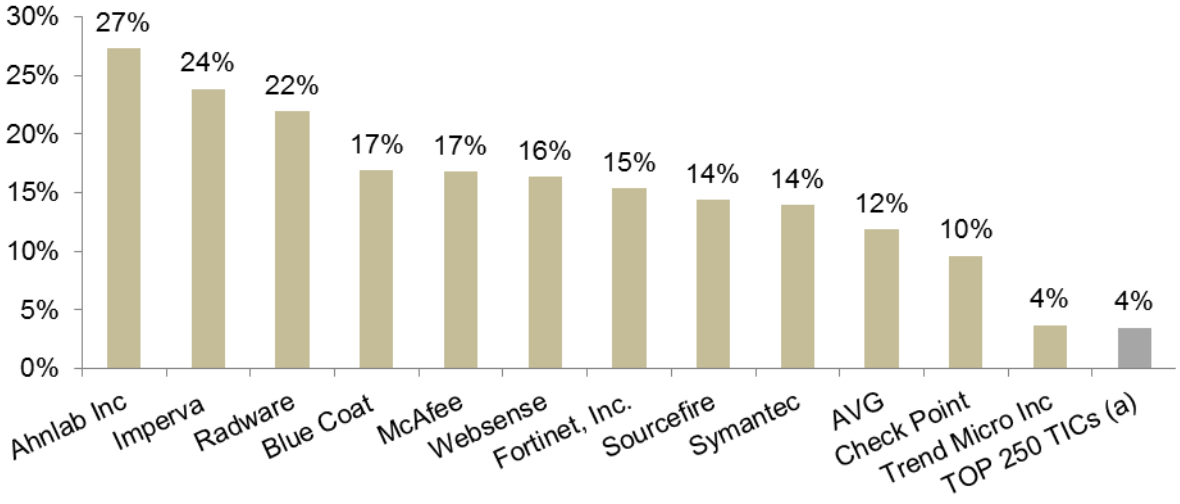
a) Nível de oportunidade

Ao analisar a dimensão de nível de oportunidade que indica a probabilidade de inovar para determinada quantidade de recurso investido em P&D, observa-se que elevados níveis de oportunidade, encontradas no setor de segurança da informação, resultam em incentivos para novas oportunidades inovativas. De maneira que, a observação de evidências de intensidade de P&D se caracteriza como uma forma adequada de medir o nível de oportunidade do setor.

No entanto, destaca-se como um limitador para existência de um indicador de intensidade de P&D global exclusivo para segurança da informação, o fato de que muitas das empresas não reportam em seus demonstrativos de resultado os investimentos em P&D, como é o caso da empresa Kaspersky Lab, que possuir 3% de participação do mercado global (OECD, 2012).

Diante disso, a (FIGURA 1) a seguir, apresenta uma das evidências de intensidade em pesquisa através da relação percentual dos investimentos em P&D e receita de vendas de empresas selecionadas, cujo foco principal (*core business*), está voltado à segurança da informação. E compara com a média do mesmo indicador das principais 250 companhias de TIC. A relevância da comparação com essas empresas de TIC provém do resultado das pesquisas realizadas pela OCDE (2008b, 2010b), que indicam que a segurança da informação é listada como prioridade para investimentos de P&D no setor.

FIGURA 1 - INVESTIMENTOS EM P&D - *(Relação percentual da receita)*



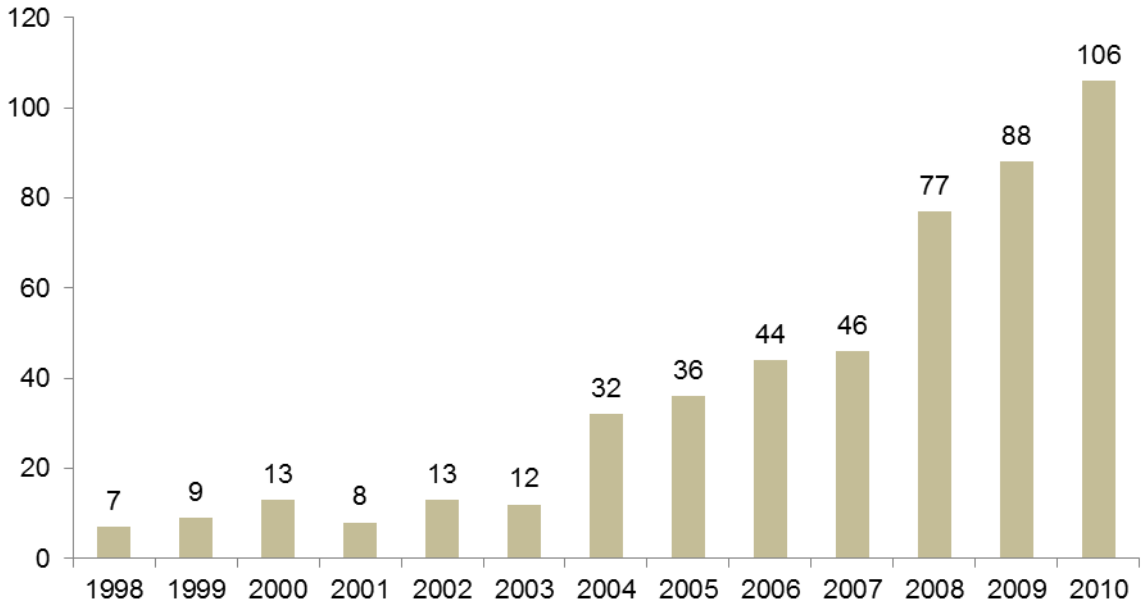
Fonte: OCDE, 2012

Empresas de SI selecionadas versus TOP 250 empresas de TICs
a)Principais empresas de TICs, conforme OCDE (2008b; 2010b)

Contudo, observa-se na FIGURA 1, que o indicador varia entre as empresas de TI de segurança de diferentes tamanhos. Das empresas selecionadas, as maiores empresas do mercado em termos de receita anual de 2010 são Symantec com mais de US$ 6 bilhões em 2010, seguido pelo McAfee, US$ 2 bilhões e Trend Micro, com US$ 1 bilhão e as demais empresas possuem faturamento inferior a US$ 1 bilhão, conforme dados extraídos do CSI Market (2014). Desta maneira, a partir desta comparação, permite concluir que o investimento em P&D de segurança da informação é superior que a média das 250 maiores empresas de TICs, sugerindo que o setor de segurança da informação é intensivo em P&D.

Adicionalmente as aquisições de empresas de segurança da informação realizadas no próprio setor e por empresas de TI, colaboram para o entendimento de que o elevado dispêndio em P&D tem alcançado resultados em termos de atividades inovativas, atraindo o interesse pela compra das empresas. A FIGURA 2 demonstra a evolução do número de aquisições de empresas de segurança da informação realizadas entre os anos de 1998 e 2010.

FIGURA 2 - AQUISIÇÕES DE EMPRESAS DE SEGURANÇA DA INFORMAÇÃO



Fonte: Tomson SDC em Khansa (2008) e PWC (2012)

A justificativa é que grandes empresas do setor de TI como IBM, Cisco, Microsoft, EMC entre outras, começaram adquirir empresas de menor porte que haviam se especializado, refletindo o crescimento da importância desse mercado para a economia. Concordando com o argumento de Stieglitz e Heine (2007) que ativos complementares são cruciais para impulsionar inovações.

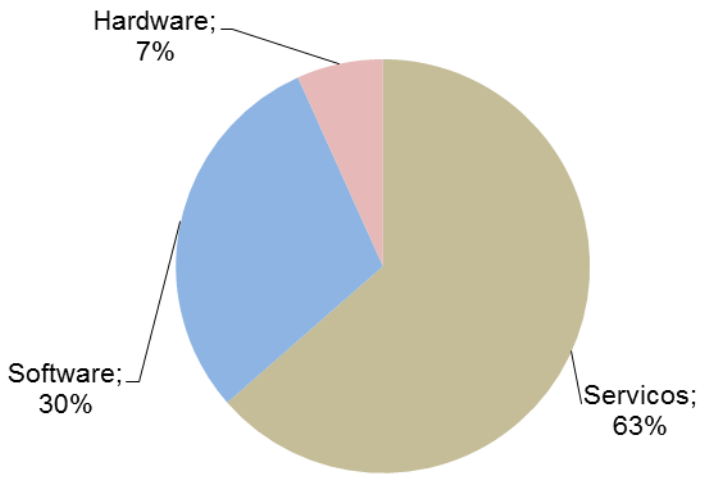
b) Variedade

Contribuindo com a avaliação das condições de oportunidade, a ampla variedade das soluções tecnológicas desenvolvidas no setor de segurança da informação tem ampla aplicabilidade em outros produtos e mercados e contribui para o surgimento de inovações. Soluções para segurança de hardware, segurança de software e serviços de segurança são muitas vezes indispensáveis para implementar outras tecnologias. Produtos e serviços desenvolvidos no setor de segurança da informação permeiam as atividades econômicas por meio de recursos tecnológicos como

a computação móvel, o *e-commerce e* o *e-bank*, amplamente adotados por diversos setores.

Conforme FIGURA 3, o segmento mais representativo de segurança da informação é atualmente o de serviços de segurança com 63% do mercado global de segurança, seguido por segurança de software, com 20% e 7% do segmento de segurança de hardware:

FIGURA 3 - PARTICIPAÇÃO GLOBAL DO MERCADO DE SEGURANÇA DA INFORMAÇÃO - *(Proporção da receita de 2013)*



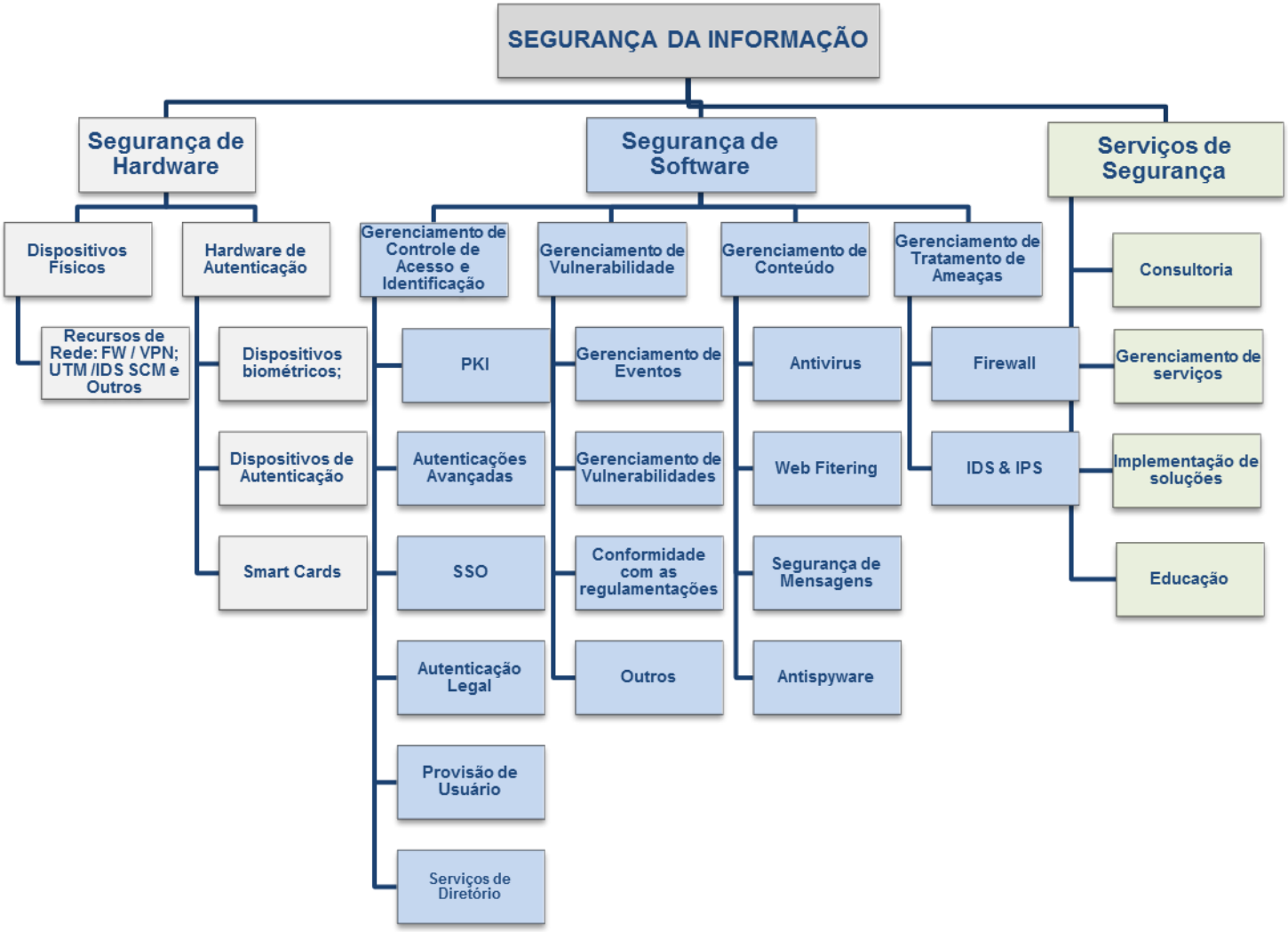
Fonte: Gartner, 2014

I)Variedade de produtos e serviços

O segmento de serviços de segurança possui por dois principais grupos: um composto por grandes empresas de TI que ofertam soluções de segurança de hardware, software e serviços. E outro por grandes companhias de auditoria e consultoria que orientam as empresas na definição de políticas, na análise de risco e na adoção de padronizações e certificações. Já o segmento de segurança de software é o que contempla maior variedade de produtos, como gerenciamento de controle de acesso e identificação, onde são aplicados os recursos de criptografia,

protocolos, certificados digitais, gerenciamento de vulnerabilidades, gerenciamento de conteúdo e de tratamento de ameaças (códigos maliciosos, vírus). Enquanto que a segurança de hardware preocupa-se com soluções de segurança de rede, VPN, firewall, hardwares de autenticação (ex.:tokens), smartcards e dispositivos para biometria. A FIGURA 4 representa graficamente a variedade de protutos e serviços desse mercado:

FIGURA 4 - VARIEDADE DE PRODUTOS E SERVIÇOS DO SETOR DE SEGURANÇA DA INFORMAÇÃO



Fonte: IDC em INTECO, 2009.

II) Ampla aplicabilidade em produtos e mercados

Os produtos e serviços de segurança da informação acima citados apresentam aplicabilidade em uma ampla gama de produtos e mercados da economia. A aplicação em dispositivos móveis, no e-commerce e no e-*banking* podem ser citados como exemplos caracterizados pela ampla utilização de recursos de segurança e pela grande propagação em diversos mercados.

a)Mobile

A proliferação dos dispositivos móveis aumentou consideravelmente a demanda por segurança e privacidade. A utilização dos dispositivos pessoais em tarefas corporativas gerou o termo BYOD - *Bring Your Own Device* (trazendo seu próprio dispositivo) (CSA, 2014). Assim, a questão da segurança não está apenas em garantir a proteção dos dados das empresas, mas também assegurar que empresa não tenha gestão sobre os dados pessoais daqueles que utilizam seus próprios dispositivos a serviço do negócio.

As soluções de segurança da informação para utilização destes dispositivos consideram o emprego de softwares específicos de segurança para *mobile*, especialmente para gerenciamento de controle acesso e identificação e soluções do segmento de serviços de segurança para garantir a criação e o monitoramento de políticas do uso de *mobile*.

b)E-commerce

No e-commerce a segurança desempenha um papel crucial frente às ameaças que visam interferir nas negociações realizadas na internet. Trata-se de códigos maliciosos, que causam indisponibilidade de serviço, destruição ou modificação de informações. São conhecidos como Vírus, Cavalo de Tróia (ou *Trojans*) e pragas virtuais que capturam senhas, roubam informações que trafegam na rede (como códigos e senhas de acesso) e spoofing de endereços de IP, que forjam o endereço de um website para simular um site oficial, entre outras ameaças.

Nesse ambiente, as soluções tecnológicas dos três segmentos são amplamente empregadas, especialmente pela contratação de serviços de monitoramento de transações que garante a possibilidade de rastrear os ataques e o tratar das ameaças. E pela utilização de softwares, como protocolos, certificados digitais entre outros que garantem autenticação do usuário via chave pública associada a uma autoridade certificadora. Além disso, alguns setores da economia como, setor financeiro, setor público (incluindo agências militares) e o setor de saúde, utilizam-se de recursos de segurança de hardware como rede remota e dispositivos de hardware para operar.

c)E-banking

O e-*banking* consiste em canais de relacionamento bancários que garantem à instituição financeira a entrega de produtos e serviços bancários tradicionais e novos ao cliente por meio de canais de comunicação eletrônicos e interativos como a internet, *smartphones* e ATMs. No caso do internet *banking* tanto as variedade de ameaças existentes, quanto as soluções tecnológicas disponíveis são similares às do e-commerce, conforme visto anteriormente. No entanto, a diferença aparece na utilização de segurança de hardware com o uso de *tokens* entre outras customizações que são motivadas pelo fato do setor financeiro ser muito visado por organizações criminosas. Outra solução de segurança de hardware que aparece no e-

banking é aplicada nos terminais ATMs por meio de dispositivos de biometria que garantem o gerenciamento de controle de acesso e identificação do usuário, como leitores de impressões digitais, palma da mão e íris.

c) Capilaridade

Conforme os parâmetros definidos por Malerba (2007), a capilaridade refere-se à aplicabilidade dos novos conhecimentos tecnológicos do setor de segurança da informação em outros produtos e mercados da economia. Ao considerar as definições apresentadas na seção 3.1 deste trabalho, que colaboram para uma interpretação que a preocupação da segurança da informação vai além da proteção computacional, buscando assim, a proteção da informação das ameaças à integridade, disponibilidade e confidencialidade da organização, a fim de garantir a continuidade do negócio e minimizar os riscos. É possível então, dizer que os conhecimentos tecnológicos desenvolvidos no campo da segurança da informação têm sido amplamente aplicados nas necessidades e oportunidades de diversos produtos e serviços e modelos negócios.

As oportunidades tecnológicas do setor surgem diante da identificação e da busca pelo tratamento de ameaças e vulnerabilidades dos modelos de negócios, que vão além do desenvolvimento de softwares e hardwares, como os modelos de gerenciamento de conformidade com regulamentações e soluções de produtos e serviços customizados para diversos modelos de negócios.

d) Fontes

A dimensão de fontes de oportunidades tecnológicas do setor de segurança da informação se refere à origem destas oportunidades do setor, podendo ser relacionada com avanços científicos em universidades, em P&D, aprendizado endógeno ou a partir de fornecedores e clientes.

De modo geral, o setor de segurança da informação possui diferentes fontes de oportunidades tecnológicas. Os avanços científicos da criptografia em universidades dos EUA como Stanford University e MIT como em laboratórios de P&D de empresas como IBM e RSA nos anos 1970 e 1980 foram cruciais para o surgimento de oportunidades no campo da segurança da informação. Esses avanços permitiram a o desenvolvimento da indústria de software de segurança da informação através de-da aplicação desses logaritmos criptográficos. Além disso, no contexto histórico é possível observar que a demanda por segurança de setores específicos da economia, como o setor financeiro, por exemplo, contribuíram para o avanço técnico.

O primeiro salto no campo da criptografia em ambiente digital ocorreu mediante a introdução dos *ATMs (Automated Teller Machine)* ou caixa automático no setor bancário. O *ATM*, além de ser considerado um marco para a história da automação foi essencial para a difusão da criptografia em outras indústrias. Em 1967 o Barckays Bank introduziu o primeiro *ATMs* produzido pela companhia inglesa Chubb. Entretanto o modelo não prosperou principalmente por falhas de segurança, pois a criptografia não era aplicada nos equipamentos. Nesse período os bancos comerciais dos EUA demandaram para a IBM o desenvolvimento de um sistema que criptografasse as mensagens de comunicação entre o ATM e os computadores centrais, os mainframes (COPPERSMITH, 1994).

Assim a IBM desenvolveu o algoritmo que culminou na cifra DES[6] (*Data Encryption Standard*), que permitiu que os *ATMs* fossem operados com maior segurança e ganhassem escala. Após este *feedback* positivo, a criptografia passou a ser adotada em outras tecnologias do setor financeiro, como os leitores de cartões tanto de agências bancárias, as maquinetas de cartão de varejo, as chamadas POS (Point of Sale) e consequentemente exerceu importante influência nos novos meios e pagamento via cartão.

Dessa forma, o controle de acesso passou a ser vista como uma das prioridades da área de TI. Como a IBM dominava o mercado de mainframe e conhecia bem as necessidades de um dos principais compradores do equipamento, que era o setor financeiro, percebeu que o setor seria um mercado com grande potencial para o desenvolvimento de um software que conseguisse centralizar o processamento da

[6] O DES (*Data Encryption Standard*) foi aprovado pelo NBS (National Bureau of Standards), atualmente NIST (*National Institute of Standards and Technology*) em 1976 como FIPS (*Federal Information Processing Standards*).

segurança (TRIPP, 2006). Lançando assim, em 1976, o software de controle de acesso, chamado RACF (Resource Access Control Facility), que atendia os requerimentos de identificação e verificação de usuários do sistema (SINGH, 2001).

3.3.2 Base de conhecimento

De acordo com Malerba (2007), a propriedades de base de conhecimento indica em que as atividades inovativas se baseiam. Sendo necessário observar duas características do setor para identificá-las: a natureza do conhecimento e dos meios de transmissão.

A característica da natureza do conhecimento tecnológico do setor de segurança da informação envolve diferentes graus de especificidade. Devido à complexidade da linguagem e da ampla gama de produtos e serviços, conforme citado na seção 3.1 b, nota-se no setor de segurança da informação a existência de padronizações (ISO, IEC, NIST, ENISA entre outras), colabora para uma interpretação de que o conhecimento é codificado. No entanto, é possível observar elementos de tacitividade em algumas circunstâncias. Com a proximidade dos fornecedores e clientes no desenvolvimento de novas soluções, improvisos motivados por customizações, sejam de softwares, hardware ou serviços, que não são documentados e geram dificuldade para transmissão do conhecimento. Essas características de tacitividade são mais evidentes no segmento de serviços. Como mencionado na seção 3.1b, que compreende atividades de consultoria, gerenciamento de segurança, treinamento e educação.

Outra característica clara do conhecimento tecnológico do setor é a interdependência do conhecimento, que presume que o elemento de conhecimento faz parte de um sistema e seu significado assume o real valor quando a tecnologia é aplicada nesse contexto (MARSILI, 1999).

Portanto, os elementos de conhecimento codificado acima mencionados refletem a característica de meios de transmissão formal (publicações, licenças, patentes) que o setor possui. Já os elementos de tacitividade, refletem os meios informais

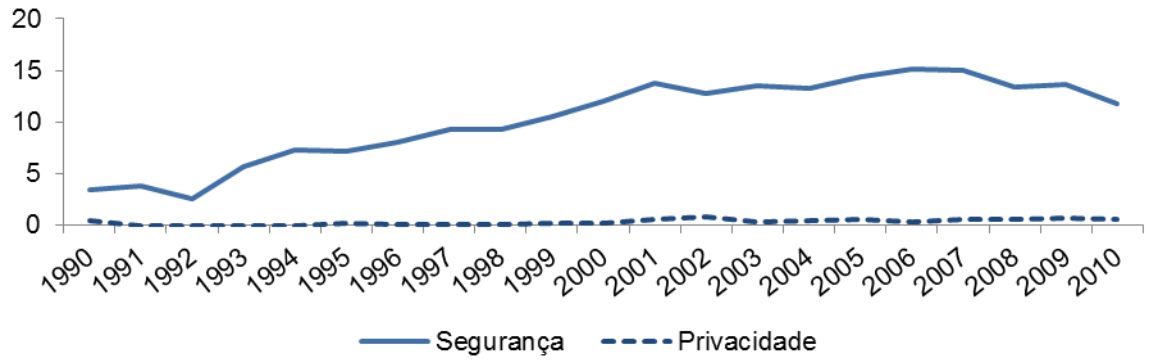
(soluções não registradas, conhecimento transmitido por meio de uma conversa) do conhecimento do setor.

3.3.3 Apropriabilidade

A propriedade de apropriabilidade indica as possibilidades de proteger as inovações de imitações e de obtenção de lucros das atividades inovadoras. Podendo ser dimensionada pelo nível de apropriabilidade e pelas características dos meios de apropriação. Sendo que o setor de segurança da informação apresenta para alguns segmentos alta apropriabilidade e para outros baixa apropriabilidade. Assim como apresenta diversidade dos meios de apropriabilidade, como analisado a seguir.

Como um resultado do processo de P&D, as patentes caracterizam-se pelo registro da atividade inventiva. No setor de segurança da informação o nível de patente cresce numa velocidade maior do que a do setor de TIC como um todo, conforme FIGURA 5 que demonstra a evolução do número das patentes de segurança e privacidade para cada 1000 patentes de TICs. Cabendo ressaltar que as invenções servem de referencial, mas não é possível garantir que as invenções se tornam inovações.

FIGURA 5 – NÚMERO RELATIVO DE PATENTES PARA SEGURANÇA DA INFORMAÇÃO – *(Por 1000 patentes de TICs)*



Fonte: OCDE, 2012

*Pedidos de patentes de **Segurança** foram identificados pelas palavras-chave: recuperação, vírus e spyware. Enquanto que as de **Privacidade** foram identificadas por identidade e privacidade.*

Os pedidos de patentes de segurança apresentadas na figura acima foram identificados a partir das palavras-chave: recuperação, vírus e spyware. Enquanto que os pedidos de privacidade pelas palavras-chave: identidade e privacidade. Ambas remetem ao segmento de software. No entanto a justificativa para uma menor proporção de pedidos de patentes para o campo de identidade e privacidade é que estas tecnologias estão baseadas no conhecimento da criptografia, que é um conhecimento codificado, conseqüentemente mais difícil de proteger. Nas décadas de 1980 e 1990 ocorreram algumas disputas judiciais, como o caso do protocolo de SSL de criptografia, considerado um dos principais mecanismos de segurança da informação, que duas empresas encubadas em grandes universidades americanas RSA (do MIT) e Cylink (de Stanford) disputaram a posse do registro. A RSA saiu vencedora. No entanto, as tecnologias de criptografia desenvolvidas nesse período expiraram no início dos anos 2000, transformaram-se em padrões que podem ser utilizados sem a necessidade do pagamento de taxas de licenciamento e convivem com algumas técnicas que são exploradas por meio de pagamento de royalties.

Embora a figura acima demonstre um aumento relativo do número de patentes em relação as patentes de TICs, não é possível afirmar que o nível de apropriabilidade do setor de segurança da informação é alto. No entanto, a partir da características dos produtos de cada segmento e da base de conhecimento é possível avaliar tanto o nível quantos os meios de apropriabilidade.

Os produtos de hardware como *tokens*, *smartcards*, dispositivos de físicos de rede apresentam características que possibilitam a imitação com maior facilidade. Já no segmento de software, os desenvolvimentos que envolvem os produtos ofertados são mais complexos e demandam maior tempo para serem copiados. Por fim, o segmento de serviços apresenta baixas condições de proteção contra imitações. No entanto, o conhecimento tácito, fruto da proximidade com clientes e de improvisos no desenvolvimento te soluções para clientes específicos, tornam o segmento dividido entre baixa e alta apropriabilidade.

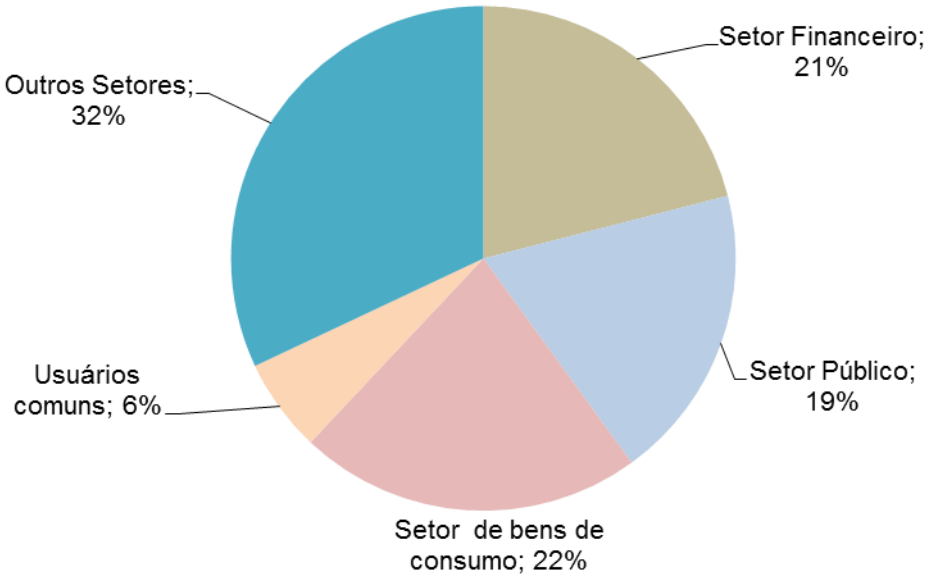
3.3.4 Cumulatividade

À cumulatividade compete indicar se o surgimento de inovações no futuro está associado a inovações realizadas no passado. Segundo Malerba (2007) uma inovação gera um fluxo de inovações posteriores, produzindo melhoria gradual ou original, ou criando novos conhecimentos que serão utilizados em outras inovações em outras áreas. A avaliação dessa propriedade se dá pela análise das fontes de comulatividade identificadas por: processo de aprendizado, fontes organizacionais e sucesso anterior.

As fontes de processo de aprendizado identificadas no setor de segurança da informação indicam que o setor adquire novos conhecimentos por meio da observação de outros conhecimentos aplicados em inovações anteriores, podendo citar a evolução da criptografia que incorporou novas soluções a partir do conhecimento existente. Assim como os as ferramentas antimalware não são descartadas com o surgimento de uma nova.

A cumultatividade do setor de segurança da informação tem origem nas instalações de P&D e especialmente no processo de aprendizagem citado acima. O monitoramento do comportamento e da evolução das ameaças e dos feedbacks críticos do mercado sobre produtos específicos por meio de ferramentas como o big data são capazes de oferecer novos conhecimentos que elevam as oportunidades de realizar inovações no setor. Sejam estas inovação para o mercado global ou para mercados específicos, como o exemplo do setor financeiro que é considerado um grande mercado para o setor de segurança da informação. Conforme a FIGURA 6, o setor corresponde a 21% do mercado.

FIGURA 6 – PARTICIPAÇÃO DO SETOR GLOBAL DE SEGURANÇA DA INFORMAÇÃO - *(% da Receita)*



Fonte: Statista, 2009

Dessa forma, a análise das propriedades acima apresentadas conduz à interpretação de que o regime tecnológico do setor, estabelecido pela combinação das propriedades da tecnologia, constitui um ambiente próspero para o surgimento de oportunidades de realizar atividades inovativas.

Observa-se também que a busca das empresas por ofertar produtos inovadores no setor, tem origem no aumento das vulnerabilidades e na sofisticação dos métodos de ataques, no contínuo surgimento de inovações tecnológicas, e na necessidade de estar em conformidade com regulamentações de diversos mercados.

A interpretação referente a observação acima, concorda com a afirmação de Kansa (2007) que a maioria das inovações em segurança da informação decorre da demanda.

Conclui-se então, que as oportunidades de gerar inovações no setor surgem como respostas aos problemas identificados pelo mercado consumidor dessas tecnologias. Sendo assim, conforme observado no referencial teórico deste trabalho, Dosi (1984) caracteriza como *demand pull*, quando as inovações tecnológicas são determinas de forma reativa.

Desta forma, sendo o setor segurança da informação guiado pelas demandas que surgem no mercado, o capítulo seguinte buscará responder como o setor financeiro, sendo um dos setores que mais utiliza tecnologias de produtos e serviços de segurança da informação, (vide figura 6), tem demandado inovações neste setor.

4 O SETOR DA SEGURANÇA DA INFORMAÇÃO A PARTIR DAS DEMANDAS DO SETOR FINANCEIRO

O aumento expressivo dos ataques e ameaças que rondam o espaço cibernético é facilmente associado às vulnerabilidades e falhas de sistemas ou de usuários que realizam transações financeiras através da internet. Podendo ser relacionadas ao gerenciamento de investimentos, contas bancárias, pagamentos de cartões de crédito ou transações de *e-commerce.* Soma-se a este fator, o contínuo surgimento de inovações tecnológicas, e a necessidade de estar em conformidade com regulamentações de diversos mercados. Estes fatores surgem como elementos fundamentais para o entendimento da importância que os mecanismos de segurança da informação, como identificação, gerenciamento de acesso, entre outros, ganharam para a realização de atividades em ambiente virtual.

Assim o setor de segurança da informação tem se desenvolvido, desde o surgimento dos computadores, tendo como objetivo garantir a privacidade, integridade e confidencialidade da informação. Ao longo dos anos, os mecanismos antigos e simplificados de criptografia foram transformados em algoritmos complexos e outras tecnologias foram desenvolvidas para atender a necessidade dos diferentes modelos de negócios que utilizam tecnologias de informação e comunicação.

Sendo assim, neste capítulo serão apresentados os elementos que demonstram como a atividade inovativa no mercado de segurança da informação tem sido orientada por demandas do setor financeiro no desenvolvimento de novas tecnologias para combater as ameaças no mundo cibernético, observando os aspectos de *demand-pull* de Dosi (1984). Para isso, o capítulo está subdividido em três seções. A primeira que retrata o período da utilização comercial dos computadores até os anos 1990, período marcado pelo desenvolvimento da criptografia em ambiente digital e o surgimento das primeiras ferramentas de autenticação. A segunda, que apresenta período da segurança da informação com o advento da internet e o contexto atual do desenvolvimento das principais tecnologias da informação e comunicação, amplamente utilizadas pelo setor financeiro.

4.1 O SURGIMENTO DA SEGURANÇA DA INFORMAÇÃO NO SETOR FINANCEIRO

Conforme visto na seção 3.2 do capítulo anterior, a principal preocupação da segurança da informação quando surgiram os primeiros mainframes residia no campo da confiabilidade dos computadores e no controle de acesso físico aos equipamentos. Apenas grandes corporações podiam adquirir um mainframe, devido ao seu alto valor. O setor financeiro foi um dos primeiros setores, juntamente com os militares e o setor aeroespacial a adotar os mainframes. O feedback positivo do uso da tecnologia, em termos de aumento de eficiência na gestão, e especialmente das transações de *back-office* determinou a difusão para outros setores da economia, tais como: farmacêutico e petroquímico (FRISCHTAK, 1992).

Conforme já relatado no capítulo 3, o primeiro salto no campo da criptografia em ambiente digital ocorreu mediante a introdução dos ATMs (Automated Teller Machine) ou caixa automático no setor bancário. Em 1967 o Barckays Bank introduziu o primeiro ATMs produzido pela companhia inglesa Chubb. No entanto, o modelo não prosperou principalmente por apresentar falhas de segurança, pois a criptografia não era aplicada nos equipamentos (COPPERSMITH, 1994).

Assim a IBM desenvolveu o algoritmo que culminou na cifra DES (*Data Encryption Standard*), que permitiu que os *ATMs* fossem operados com maior segurança e ganhassem escala. Após este *feedback* positivo, a criptografia passou a ser adotada em outras tecnologias do setor financeiro, como os leitores de cartões tanto de agências bancárias, em maquinetas de cartão de varejo, chamadas POS (Point of Sale) e consequentemente exerceu importante influência nos novos meios e pagamento via cartão.

Nos anos 1970, o aumento do uso dos mainframes pelo setor financeiro, e por conseqüência do número de usuários que tinham acesso às aplicações disponíveis gerou a busca por controle de acesso e identificação desses usuários. A proximidade entre a IBM e seus clientes do setor financeiro permitiu o desenvolvimento de ferramentas para suprir essa demanda (TRIPP, 2006). Lançando assim, em 1976, o software de controle de acesso, chamado RACF (Resource Access Control Facility), que atendia os requerimentos de identificação e verificação de usuários do

sistema. Assim o controle de acesso passou a ser visto como uma das prioridades da área de TI (SINGH, 2001).

A aplicação dos novos controles de acesso teve grande valia diante da inserção dos minicomputadores. Estes representaram importante progresso na área da automação bancária no final da década de 1970. O principal papel dos minicomputadores era o de capturar e armazenar os dados primários em agências bancárias antes do envio das informações para os grandes CPDs – Centro de Processamento de Dados (FONSECA, MEIRELES E DINIZ, 2010, p.137). Esses novos controles foram essenciais para o desenvolvimento das áreas de *back-office*, garantindo redução de riscos operacionais.

Nota-se, no contexto acima, que o surgimento dessas duas inovações (DES, RAFC) caracteriza a resposta do então jovem setor de segurança da informação aos problemas identificados pelo setor financeiro, indo de encontro com o objetivo geral do trabalho.

4.2 A SEGURANÇA DA INFORMAÇÃO E AS RECENTES MUDANÇAS TECNOLÓGICAS

4.2.1 Internet banking

A partir da introdução da internet nos anos 1990 no meio comercial a área de segurança da informação passou a ganhar maior importância. O comércio eletrônico expandiu-se rapidamente acompanhado de uma gama de oportunidades e desafios para TI. Muitas das ameaças passaram a atingir diversos setores da economia, especialmente o setor financeiro, onde as organizações criminosas encontraram o maior conjunto de atrativos para desenvolver os sofisticados mecanismos de fraude eletrônica.

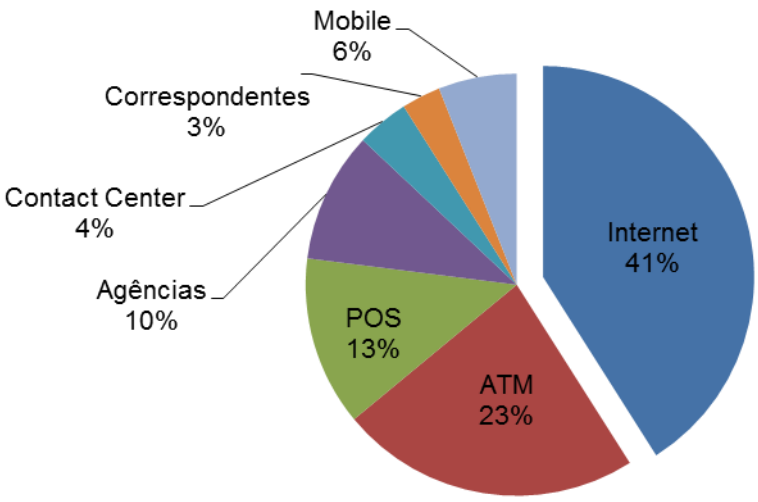
Inicialmente os bancos perceberam a popularidade da *internet* e a utilizaram apenas como propaganda dos seus produtos e serviços. Isso porque os websites eram estáticos. A busca das empresas e por realizar negócios através da *internet*,

como compra de mercadorias com cartão de crédito e transações online, levou a Netscape a lançar o protocolo de segurança SSL (Secure Socket Layer), conforme visto na seção 3.2 do capítulo anterior, que garantiu o desenvolvimento da *internet*, e consequentemente do *internet banking.* Segundo Adachi (2004), o banco Security First Network Bank foi o primeiro banco nos EUA a oferecer aos seus clientes o acesso às contas e a realização de pagamentos.

Assim, conforme relata Adachi (2004), cerca de cinco anos foram suficientes para a difusão dos feedbacks positivos da nova ferramenta em comparações com o banco físico. Assim, o início do século 21 passou a contar com praticamente todos os bancos comerciais das economias desenvolvidas operando em plataforma on-line.

Nesse período, o novo modelo de *internet banking* evoluiu para um importante canal de relacionamento em expansão. Segundo relatório da FEBRABAN, 2014, as transações realizadas por este canal correspondem a 41% do total de 40,2 bilhões de transações bancárias realizadas em 2013, conforme demonstra a FIGURA 7 a seguir.

FIGURA 7 - TRANSAÇÕES BANCÁRIAS POR CANAL DE ATUAÇÃO (%) -



2013

FONTE: FEBRABAN: 2014

Dessa forma, a nítida importância da ferramenta para o atual modelo de negócio, e os riscos associados à utilização da *internet* elevaram a demanda por uma

gestão ainda mais eficiente da segurança da informação. Conforme Damiano (2013) o desafio de TI que até então estava em oferecer à corporação à integração das ferramentas de identificação e acesso, passou a contemplar a demanda por respostas rápidas e eficientes às vulnerabilidades que surgiam constantemente e também as mudanças organizacionais promovidas pela adoção das novas tecnologias da informação.

Assim, conforme Fonseca, Meireles e Diniz (2010), a segurança da informação passou então a ser encarada pelos bancos não só como meio de minimizar os riscos estratégicos, financeiros e operacionais, mas também como um importante aspecto de coesão de gestão entre as áreas de negócio e tecnologia.

Nesse contexto, em que o campo da segurança da informação ganhou extrema importância no setor financeiro, conforme definições do anexo 1.

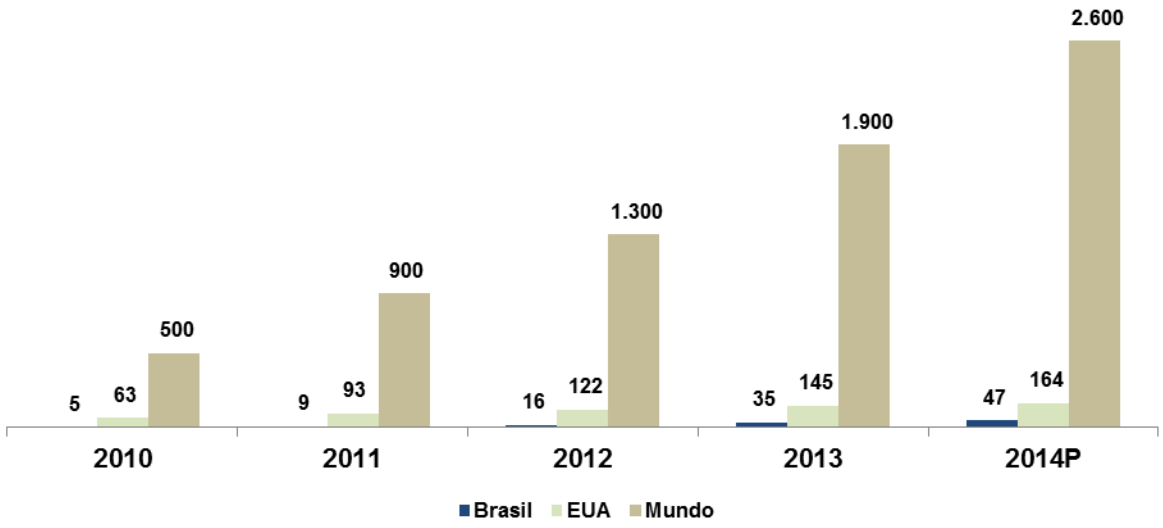
A partir dessa evolução do *internet* banking como canal de relacionamento bancário, observa-se que os avanços tecnológicos são impulsionados pelas soluções de problemas de segurança do setor de financeiro. E obedecem a um processo, que simplificadamente pode ser descrito: Diante da necessidade de oferecer novos produtos para os seus clientes, os bancos avaliam as condições de segurança desse produto. Ao identificar os problemas de segurança da informação, os bancos recorrem aos seus fornecedores de tecnologia para demandar soluções. Resultando no surgimento de inovações por meio de novas tecnologias ou melhoramentos de tecnologias existentes.

4.2.2 *Mobile Banking*

A computação móvel, chamada no contexto bancário de *mobile*, representada especialmente pela ampla difusão dos *smartphones* e também dos *tablets*, tem se destacado como um importante canal de relacionamento bancário nos últimos anos, *e*specialmente por garantir ao cliente a possibilidade de acesso às transações bancárias sem restrição de localização. Em 2013 já existiam 1,9 bilhões de smartphones em todo mundo conforme levantamento obtido do instituto de pesquisa

IDC (2014). A com expectativa de 2,6 bilhões dispositivos em 2014, conforme FIGURA 8 a seguir:

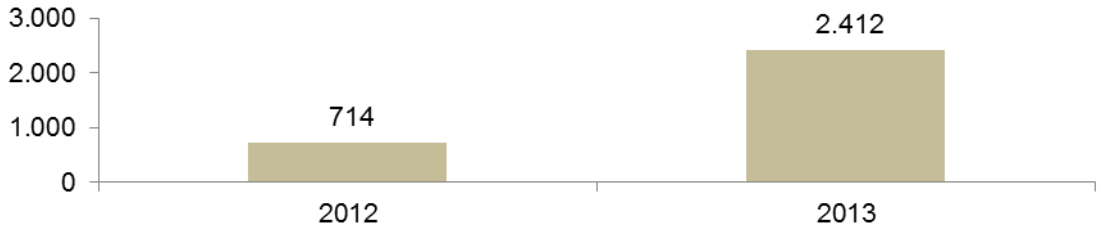
FIGURA 8 – NÚMERO DE *SMARTPHONES - (Em milhões de unidades)*



Fonte: IDC, 2014

Segundo a FEBRABAN (2013) a introdução dos dispositivos móveis como um canal bancário, denominado *mobile bank,* ocorreu no mercado brasileiro em 2012. O total de transações bancárias realizadas por meio desta modalidade representava apenas 2% do total, cerca de 714 milhões de transações bancárias. Em 2013 o canal expandiu expressivamente para 2,4 bilhões de transações, conforme FIGURA 9 a seguir.

FIGURA 9 - NÚMERO DE TRANSAÇÕES REALIZADAS PELO CANAL MOBILE BANK - (em milhares)



FONTE: FEBRABAN, 2014

No entanto a tecnologia também se destaca pelos desafios que a acompanham no campo da segurança. O aumento dos níveis de ameaças, em termos de volume e de sofisticação, por meio de malwares,criados especificamente para afetar esse tipo de dispositivo, representam potenciais prejuízos financeiros e de reputação, assim como a maior utilização de dispositivos pessoais em uso corporativo que caracterizam o conceito BYOD também exigem das áreas de TI dos bancos uma atuação peculiar. Pois dispositivos infectados por vírus ou cavalo de tróia podem afetar a rede corporativa dos bancos (KAPERSKY, 2012).

Devido à importância que o canal representa para os bancos, a demanda por soluções de segurança tem aumentado. Por isso, novas tecnologias para mobile tem surgido para atender essas demandas como, softwares de segurança específicos para mobile, antivírus, dispositivos de leitura de impressões digitais no próprio aparelho e reconhecimento facial, entre outros.

De acordo com uma pesquisa realizada nos EUA pelo Federal Reserve (2013), 48% da amostra de 2.290 entrevistados que utilizam *smartphones* possui alguma preocupação sobre o nível de segurança ao utilizar o *mobile bank*. E 42% deixaram de realizar pagamentos via *mobile bank* devido a preocupações com segurança.

Além disso, o segmento de segurança para mobile tem crescido. Segundo a MarketWatch, (2014), estima-se que o mercado tenha crescido de 119% de 2012 para 2013, conforme FIGURA 10.

FIGURA 10 - SEGMENTO DE SEGURANÇA PARA *MOBILE* GLOBAL (*em bilhões de US$*)

Fonte: Marketwatch, 2014

(*) dados estimados pela consultoria especialista em análise desse mercado.

Levando em conta as evidências acima, tanto do contexto do setor financeiro, quanto do avanço da tecnologia de mobilidade, do resultado da pesquisa do Federal Reserve e do crescimento do mercado de segurança para mobile, é possível concluir que as oportunidades de inovar nesse segmento também possuem o mesmo padrão, sendo impulsionadas por informações do mercado.

4.2.3 *Cloud computing*

O *cloud computing* ou computação em nuvem é definida pelo NIST (2011) como um modelo que permite acesso onipresente à rede, sob demanda, a um conjunto compartilhado de recursos configuráveis de computação (por exemplo, redes, servidores, armazenamento, aplicações e serviços). Podendo ser rapidamente provisionados e liberados com um esforço mínimo de gerenciamento ou interação com o provedor de serviços. A computação em nuvem tem origem na experiência em organizar e prover recursos computacionais de empresas que constroem grandes *data centers* e ofertam estes recursos a um custo menor, devido ao ganho de escala, para qualquer modelo de negócio.

Deste modo, segundo (Garg, 2011) as principais características da cloud computing que tornam a tecnologia atrativa para as organizações em geral estão descritas nos cinco pontos abaixo:

I) Provisionamento *on-demand*: trata-se de auto-serviço ou auto-atendimento. Os recursos de banda larga, armazenamento ou rede podem ser utilizados sem interação humana com prestadores de serviços.

II) Ubiqüidade de acesso: acesso aos sistemas, independentemente da localização do usuário ou dispositivo (PC, *smartphone, tablet*, etc.)

III) Pool de recursos: os recursos computacionais da nuvem como armazenamento, processamento, memória, banda e máquinas virtuais, ficam reunidos geograficamente. O cliente não possui controle sobre a real localização dos recursos que está utilizando, tendo somente uma informação mais ampla como o país em que se encontra, o estado ou o *Data Center.*

IV) Elasticidade Rápida: é a capacidade de alocar mais ou menos recursos no momento em que for necessário e com agilidade. E pode adquirir mais ou menos recursos de acordo com a necessidade de suas aplicações.

V) Serviços Mensuráveis*:* os serviços são controlados e monitorados pelo provedor de forma transparente. Possibilitando o usuário do serviço otimizar sua utilização da nuvem.

Tendo em vista que as características acima remetem a oportunidades de ganho de eficiência, redução de custos e aumento de lucratividade para as empresas. Soma-se o fato que a computação em nuvem é essencial para aplicação de análises de big data[7], devido ao grande volume de dados não estruturados que precisam ser acessados por essas aplicações. Segundo Garg (2011), o setor financeiro tem encontrado barreiras para adoção da tecnologia no especialmente no campo da privacidade de dados, disponibilidade e falta de normas, etc.

A preocupação é que os dados tanto dos bancos como de clientes vulneráveis em nuvem pública, podendo ser utilizados por terceiro para outro fim. Podendo incorrer a implicações de reputação ou a ações judiciais de clientes. Além disso, os gestores de TI preocupam-se com a disponibilidade. Se por ventura um sistema ficar fora do ar por um dia, ou que uma base de dados seja deletada, traria uma série de complicações para a instituição.

[7] O big data tem se apresentado para o setor financeiro como um aliado para tornar os bancos mais eficientes a partir dos inúmeros cruzamentos de dados, que a partir de ferramentas de *business inteligence (BI),* permite que o comportamento dos clientes seja analisado, e novas e personalizadas soluções sejam oferecidas FEBRABAN, 2013). Além disso, a ferramenta pode ser útil na prevenção de incidentes de segurança da informação a partir da análise do comportamento dos ataques e identificação de vulnerabilidades.

A despeito dessas preocupações, o mercado de TI tem se movido em torno de modelos de implantação [8] de nuvem que podem servir de alternativa para adoção da tecnologia. A utilização da nuvem híbrida, a partir da avaliação do escopo das aplicações e da identificação das informações que não são *core business* pode representar um ganho inicial. Segundo Garg (2011) parte do Bank of America, Merrill Lynch utilizam servidores em nuvem como estratégia para construir e avaliar os programas de análise de risco. O Morgan Stanley usa nuvem para suas aplicações de análise e estratégia.

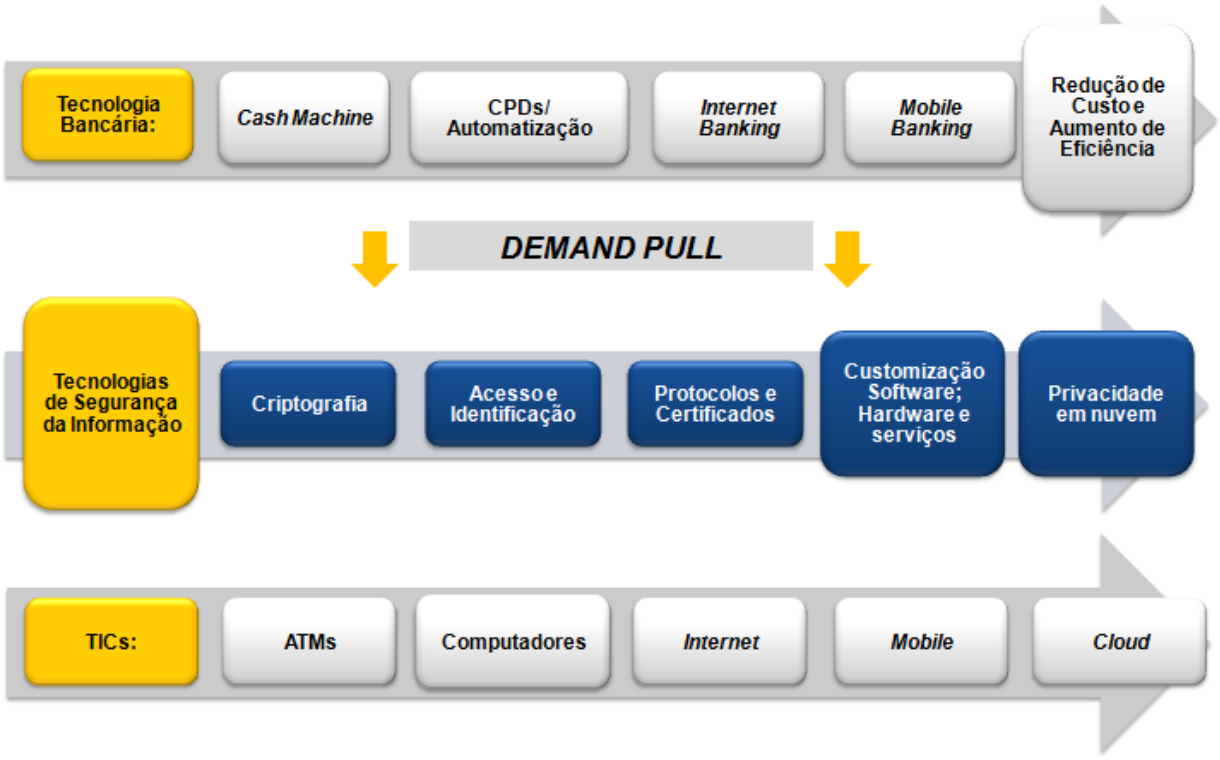
Para fazer frente a esse trabalho de avaliação de escopo, citado acima, empresas de segurança da informação, como exemplo da Microsoft Trustworthy, desenvolveram softwares que auxiliam os bancos a compreender e avaliar a infraestrutura de TI, a identificar as questões de regulamentação, e avaliar se a adoção da nuvem irá satisfazer as suas necessidades de negócios. Além disso, existe um conjunto de esforços entre universidades e empresas para desenvolver o ambiente de nuvem para minimizar a vulnerabilidade.

Contudo, o contexto da segurança da informação em relação às tecnologias de computação em nuvem, também colabora com a interpretação que o setor é direcionado pelas respostas do mercado que surgem diante das novas tecnologias.

Dessa forma a análise da evolução das tecnologias de informação e comunicação, observa-se que tais tecnologias foram utilizadas no contexto do setor financeiro depois de sofrerem adaptações que se caracterizam como inovações tecnológicas no campo da segurança da informação.

[8] O NIST (2009) apresenta três modelos de implantação da computação em nuvem: público, privado e híbrido. A computação em nuvem pública é oferecida por grandes empresas provedoras de serviços, cujos equipamentos, infra-estrutura ou aplicações são compartilhados por milhares de clientes ao redor do mundo através da internet. Nesse modelo, o armazenamento e conectividade são flexíveis, podendo ser ampliados ou reduzidos conforme as necessidades do usuário, no sistema *pay-per-use*, (pague conforme o uso). A computação em nuvem privada é um modelo de ambiente protegido onde o acesso é permitido aos seus funcionários e parceiros de negócio da empresa. Entretanto, nesse modelo há exigência de investimentos em ativos devendo ser usada quando há necessidade de níveis mais rigorosos de segurança e privacidade, ou de garantia de disponibilidade de aplicação, sem os inevitáveis atrasos de acesso via internet. Enquanto que a computação em nuvem híbrida é a junção dos dois modelos (BRICT, 2014).

FIGURA 21 – EVOLUÇÃO DAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO, TICS E TECNOLOGIA BANCÁRIA.



Fonte: Elaboração própria

Desse modo, a figura 11 apresenta as principais tecnologias abordadas no trabalho, onde é possível observar esse processo de desenvolvimento tecnológico que permite que tecnologias da informação e comunicação sejam utilizadas como tecnologias bancárias através de inovações tecnológicas no campo da segurança da informação.

5 CONSIDERAÇÕES FINAIS

A segurança da informação é um setor guiado pela demanda, e o setor financeiro é um dos principais demandantes de soluções desta área. O presente trabalho buscou apresentar como as tecnologias da segurança da informação evoluíram a partir das demandas desse setor, considerando o embasamento teórico de Dosi (1984) sobre *demand pull*.

Através da análise das propriedades dos regimes tecnológicos em Malerba e Orsenigo (1997) e Malerba (2007) específico do setor de segurança da informação, bem como das evidências das tecnologias utilizadas no setor financeiro, conclui-se que as oportunidades de inovações tecnológicas que surgem no setor de segurança da informação são respostas às necessidades de solucionar problemas de segurança do setor financeiro. Ou seja, diante da necessidade de oferecer novos produtos para os seus clientes, os bancos avaliam as condições de segurança dos produtos. Ao identificar os problemas de segurança da informação, os bancos recorrem aos seus fornecedores de tecnologia para demandar soluções. Resultando no surgimento de inovações por meio de novas tecnologias ou melhoramentos de tecnologias existentes.

Assim, através da análise da evolução das tecnologias de informação e comunicação, observa-se que tecnologias como *ATMs*, computadores, *internet*, *mobile* e computação em nuvem somente foram utilizadas no contexto do setor financeiro depois de sofrerem adaptações que se caracterizam como inovações tecnológicas no campo da segurança da informação. De modo que as evidências apresentadas ao longo do estudo demonstram que esse processo caracteriza que o setor financeiro demanda soluções tecnológicas do setor de segurança da informação para minimizar prejuízos com fraudes e aumento de eficiência.

Por fim, sugere-se que o setor de segurança da informação investigue as oportunidades de inovações por meio de tecnologias de big data, ampliando assim, as fontes de informação do setor e aumentando a capacidade preditiva sobre o comportamento dos ataques e ameaças cibernéticas. A utilização de tais tecnologias pode impactar especialmente o segmento de serviços de segurança da informação relacionados a monitoramento e gerenciamento de ameaças e ataques.

REFERÊNCIAS

ABNT, Associação Brasileira de Normas Técnicas. Tecnologia da Informação - **Código de práticas para gestão da segurança da informação**. NBR ISSO/IEC 17799:1999. Rio de janeiro, 2000.

ADACHI, T. **Gestão da segurança em *internet*: estudos de casos brasileiros**. Dissertação (mestrado) – Fundação Getúlio Vargas, São Paulo, 2004.

ANDERSON, J. ***Why we need a new definition of information security****. Computers & Security, 22(4), 308–313. Elsevier. New York, 2003.*

ANTONELLI, C...***The Economics of Innovation, New Technologies and Structural Change****. Routledge, London, 2003.*

AUERBACH INFO INC. ***Minicomputers. Pensilvania****. 1971.*Disponível em: <http://bitsavers.informatik.unistuttgart.de/pdf/auerbach/Auerbach_Minicomputers_Mar71.pdf> Acesso: 15/07/2014.

AUDRETSCH, D. ***Technological regimes, industrial demography and the evolution of industrial structure***,Industrial and Corporate Change,6 (1), 1997.

BECKER, M. ***The concept of routines twenty years after Nelson and Winter (1982): A review of the literature.*** *Danish Research Unit for Industrial Dynamics.* 2006.

BELL, G. ***Stars: Rise and Fall of Minicomputers****.* Disponível em: <http://ieeeghn.org/wiki/index.php/STARS:Rise_and_Fall_of_Minicomputers> Acesso: 21/07/2014

BRESNAHAN F.; TRAJTENBERG M. ***General purpose technologies: Engines of growth***, Journal of Econometrics, vol. 65, p. 83-108. 1995.

BRESCHI, S.E MALERBA, F. '***Sectoral innovation systems: technological regimes, Schumpeterian dynamics and spatial boundaries***', *in C. Edquist (ed.), Systems of Innovation. Technologies, Institutions and Organisations, London: Cassell. 1997.*

BRICT – Brasil ICT. **Diferença entre nuvem privada, pública e híbrida**. Disponível em: http://www.brict.com.br/cloud-virtualization/diferenca-entre-nuvem-privada-publica-e-hibrida/ Acesso: 01/09/2014

BUTTACIO.J. ***The Evolution of Cryptography - From Caesar To RSA: Investigations in the Flaws and Advantages.*** *Durham. Inglaterra. 2003*. Disponível em: http://www.cs.duke.edu/courses/spring05/cps182s/assign/project/fall03/sbh4_1/project.pdf

BRYNJOLFSSON, Erik; HITT, Lorin M. ***Beyond Computation: Information Technology, Organizational Transformation and Business Performance***, *Journal of Economic Perspectives*, Vol.14, n. 4, p. 23-48, 2000.

CIMOLI, M.; DOSI, G. : ***De los paradigmas tecnológicos a los sitemas nacionales de produccíon e innovacion.*** *Comercio exterior, vol. 44, N 8, México, D.F.,* Banco Nacional de Comercio Exterior (BANCOMEXT), 1994b.

CHERDANTSEVA, Y.; HILTON, J. ***The Evolution of Information Security Goals from the 1960s to today****.* Disponível em: https://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf Acesso: 15/05/2014.

COHEN, M. E LEVIN, R. ***'Empirical studies of innovation and market structure'****, in R. Schmalensee and R. Willig (eds), Handbook of Industrial Organisation, Amsterdam: North-Holland* ,(1989).

CONSOLI, D. ***The dynamics of technological change in UK retail banking services: na evolutionary perspective****. Research Policy 34, 4, 461-480, 2005.*

CORAZZA, R.; FRACALANZA, P. **Caminhos do pensamento neo-schumpeteriano: para além das analogias biológicas**. Nova Economia, v. 14, n. 2, p. 127-155, 2004.

COPPERSMITH, D. ***The Data Encryption Standard (DES) and its strength against attack.*** *IBM J.Res.Develop. VOL. 38 No. 3 May 1994*.Disponível em: <http://domino.watson.ibm.com/tchjr/journalindex.nsf/0/94f78816c77fc77885256bfa0067fb98?OpenDocument > Acesso: 25/06/2014.

CSI MARKET.disponível em: <http://www.csimarket.com> Acesso em: 20/09/2014.

DAMIANO, A. **As fraudes no *internet* banking e sua evolução para o social banking. Dissertação (mestrado)**. USP. São Paulo, 2013. Disponível em: http://www.teses.usp.br/teses Acesso: 12/07/2014

DEEPAK, G. *et. al*. ***Challenging Issues and Limitations of Mobile Computing***," *International Journal of Computer Technology & Applications,* Vol 3 (1), 177-181, 2012.

DIFFIE, W.; HELLMAN, M. ***New directions in cryptography. Information Theory****, IEEE Transactions on, v. 22, n. 6, p. 644-654, 1976.*

DINIZ, E. **Evolução e segmentação no perfil dos serviços bancários pela *Internet***. Relatório de pesquisa. São Paulo: FGV-EAESP, 2004.

DOSI, G. **Paradigmas tecnológicos e trajetórias tecnológicas: uma proposta de interpretação dos determinantes e direções da mudança técnica**. Science Policy Research Unit, University of Sussex, Brighton U.K., 1982.

DOSI, G. “**Mudança técnica e transformação Industrial**”. Campinas: Ed. Unicamp, 2006.

FEDERAL RESERVE. ***Mobile device report- 2013.*** Disponível em: <http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf> Acesso em: 23/10/2014

FEBRABAN - Federação Brasileira de Bancos. Disponível em: <http://www.febraban.org.br>. Acesso em: 23/03/2014.

FONSECA C.; MEIRELLES F.; DINIZ E. **Tecnologia bancária no Brasil: Uma história de conquistas, uma visão de futuro**. São Paulo. Ed.FGVRAE, 2010.

FREEMAN, C. The Economics of Industrial Innovation, London: Pinter. 1982.

FRISCHTAK, C.. **Automação bancária e mudança na produtividade: a experiência brasileira**. Pesquisa e Planejamento Econômico, Rio de Janeiro, 22, 2, 197-240, 1992.

GARG.A ***Gm Clould computing***. Disponível em: <http://www.sapient.com/content/dam/sapient/sapientglobalmarkets/pdf/thought-leadership/GM_Cloud_Computing.pdf> Acesso em: 30/10/2014

GARTNER. ***Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware.*** Disponível em: <http://www.gartner.com/newsroom/id/2828722> Acesso em: 25/08/2014

GORT, M. E KLEPPER, S. ***Time paths in the diffusion of product innovations***, *Economic , Journal*,92, 630–53, 1982.

HITCHINGS, J. ***The need for a new approach to information security.*** *In: 10th International Conference on Information Security (IFIP Sec’94). p. 23-27, 1994.*

INTECO – INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION. ***Study of the ICT security sector in Spain.*** 2009. Disponível em:< https://www.incibe.es/file/2kOaVV8KOgotSH7Apl5n5Q.> Acesso em: 25/09/2014.

KAPERSKY. ***Security Technologies for Mobile and BYOD***. Disponível em: <http://media.kaspersky.com/en/business-security/Kaspersky-Security-Technologies-Mobile-BYOD.pdf>. Acesso em: 20/08/2014

KHANSA, L.; LIGINLAL, D. ***The Influence of Regulations on Innovation in Information Security.*** *Americas Conference on Information Systems. AMCIS, 2007 Proceedings. Paper 180. Disponível em: <http://aisel.aisnet.org/amcis2007/180>,* Acesso:15/08/2014

KHANSA, L. ***Dissecting the market dynamics of the information security sector: demand-pulled innovation and industry convergence****. Ann Arbor, Michigan, ProQuest,* 2008*.*

KAHN, D. ***The Codebreakers****. New York, NY, The New American Library, Inc.*,p.64-67,1967.
KUHN, Thomas. **A estrutura das revoluções científicas**. 7. ed. São Paulo: Perpectiva, 2003.

LEVIN, R. *et. al*. ***Appropriating the Returns from Industrial Research and Development***, *Brookings Papers on Economic Activity*(3), 783-820, 1987.

LORENS, E. **Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação**. Brasília: CID/UnB, Dissertação de Mestrado de Ciências da Informação. 2007.

HAMDAGA, M.; TAHVILDARI,L. ***Cloud Computing Uncovered:A Research Landscape****. Elsevier Press.p.41-85, 2012.*

HITCHINGS, J. ***The need for a new approach to information security.*** *In: 10th International Conference on Information Security (IFIP Sec'94). p. 23-27, 1994.*

MACEDO, D. O **que é a computação forense e sua importância no âmbito empresarial**. Disponível em: <http://www.diegomacedo.com.br/o-que-e-a-computacao-forense-e-sua-importancia-no-ambito-empresarial>Acesso: 25/07/2014

MALERBA, F. ***Schumpeterian patterns of innovation and technological regimes.*** *Elgar Companion to Neo-Schumpeterian Economics. Great Britain by MPG Books Ltd, Bodmin, Cornwall,* p. 345-359, 2007.

MALERBA, F. E ORSENIGO, L. '***Technological regimes and patterns of innovation: a the-oretical and empirical investigation of the Italian case'****, in A. Heertje and M. Perlman (eds),Evolving Technologies and Market Structure, Ann Arbor, MI: Michigan University Press. 1990.*

MALERBA, F. E ORSENIGO, L. ***Technological regimes and firm behaviour,Industrial and Corporate Change****,2 (1), 45–71. 358, 1993..*

MARKETWATCH. ***Global mobile security m security market***. Disponível em: <http://www.marketwatch.com/story/> Acesso em:26/10/2014.

MARSILI, O. ***Technological regimes: theory and evidence.*** 1999. Disponível em: <http://www.lem.sssup.it/Dynacom/files/D20_0.pdf> Acesso em: 24/10/2014.

NELSON, R.; WINTER, S. ***A case study in the economics of information and coordination: the weather forecasting system****. The Quarterly Journal of Economics, p. 420-441, 1964.*

NELSON, R.; WINTER S. ***In search of useful theory of innovation.*** *Research policy 6.1 36-76; 1977.*

NELSON, R.; WINTER, S. ***An evolutionary theory of economic change.*** *Cambridge, Mass*.: Harvard University Press, 1982.

NEW YORK TIMES. ***Russian Accused of Citibank Computer Fraud***. Disponível em: <http://www.nytimes.com/1995/08/18/business/russian-accused-of-citibank-computer-fraud.html> Acesso: 28/07/2014

NIST - National Institute of Standards and Technology. ***The NIST Definition of Cloud Computing***. Disponível em: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf> Acesso: 04/06/2014

OCDE - The Organisation for Economic Co-operation and Development. ***Internet Economy Outlook 2012.*** Disponível em: http://www.oecd.org/sti/ieconomy/internet-economy-outlook-2012-highlights.pdf. Acesso em: 04/09/2014.

OCDE - The Organisation for Economic Co-operation and Development. ***Information Technology Outlook 2008(b).*** Disponível em: <http://dx.doi.org/10.1787/it_outlook-2008-en> Acesso em: 09/10/2014

OCDE - The Organisation for Economic Co-operation and Development. ***Information Technology Outlook 2010(b).*** Disponível em: < http://dx.doi.org/10.1787/it_outlook-2010-en> Acesso em: 09/10/2014

PELTIER, T. ***The practice of information security.*** *in Perspective: 20 years of security.* Disponível em: http://www.airtightnetworks.com/fileadmin/pdf/SC_magazine_Nov2009.pdf Acesso:25/07/2014

PHILIPSON, G. ***Calling a mainframe computer by any other name***. Disponível em: <http://www.smh.com.au/articles/2002/11/09/1036308526769.html> Acesso: 05/07/2014

POSSAS, M. **Em direção a um paradigma microdinâmico: a abordagem Neo-schumpeteriana.** Ensaios sobre economia política moderna: teoria e história do pensamento econômico. São Paulo: Marco Zero p.: 157-177, 1989.

PWC. ***Cyber Security M&A: Decoding deals in the global Cyber Security industry - 2011*****.** Disponível em:http://www.pwc.com/gx/en/aerospace-defence-and-security/publications/cyber-security-mergers-and-acquisitions.jhtml > Acesso em: 05/10/2014.

TRIPP, R. ***Development of IT Security*****. Disponível em:** <http://howbankswork.com/?s=Development+of+IT+Security> Acesso em: 19/07/2014.

ROSENBERG, N. ***Perspectives on technology****. New York: Cambridge University Press, 1976.*

ROSENBERG, N. ***Inside the black box: technology and economics****. New York: Cambridge University Press, 1982.*

SALTZER, H. e SCHROEDER, M. D. ***The Protection of Information in Computer Systems.*** *Proceedings of the IEEE,* 1975. 63(9), 1975.

SÊMOLA, Marcos et al. **Gestão da Segurança da informação**. Elsevier Brasil, 2003.

SINGH, S. ***The Code Book : how to make it, break it, hack it, crack it****. Delacorte Press. New York, New York. 2001.*

SCHUMPETER, J.***Capitalism, Socialism and Democracy***, New York: Harper and Brothers, 1942.

SCHUMPETER, J*.* ***Essays of J.A. Schumpeter.*** *Cambridge, MA: Addison Wesley Press, Inc., 1951*

SCHUMPETER, J. **Capitalismo Socialismo e democracia**. (Editado por George Allen e Unwin Ltd., traduzido por Ruy Jungmann). Rio de Janeiro: Editora Fundo de Cultura, 1961.

SCHUMPETER, J. **Teoria do desenvolvimento econômico: uma investigação sobre lucros, capital, crédito, juro e lucro econômico**. São Paulo. Abril Cultural, 1982

STATISTA. The Statistics Portal. Disponível em:<http://www.statista.com>. Acesso em: 01/08/2014

STIEGLITZ, N. E HEINE. K. ***Innovations and the role of complementarities in a strategic firm.*** *Strategic Management Journal,* v. 28, n.1, p.1-15, 2007.

SUMMERS, R. ***Secure computing: threats and safeguards****. New York. McGraw-Hill, 1997.*

TEECE, D. J. ***Profiting from technological innovation: Implications for integration collaboration, licensing and public policy****. Research Policy*, 15, 285-305, 1986.

TIGRE.P.. **Computadores brasileiros: indústria, tecnologia e dependência**. São Paulo: Editora Campus, 1984.

TIGRE, P. ***E-commerce readiness and diffusion: the case of Brazil. Relatório de pesquisa****, University of California at Irvine, Center for Research on Information Technology and Organizations, 2003.*

TIGRE P.; NORONHA V. **Do mainframe à nuvem: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação** R.Adm.. São Paulo, v.48, n.1, p.114-127, jan /fev /mar. 2013

THOMAS A. ***SLL & TLS Essential: Securing the Web***. Elsevier, New York, 2000.

WINTER, S. ***Economic 'natural selection' and the theory of the firm.*** *Yale Economic Essays, Vol. 4 No. 1, pp. 225-272, 1964*.

WINTER, S.G. (1984). ***Schumpeterian competition in alternative technological regimes***,*Journal of Economic Behavior and Organization*,5, 287–320.

ANEXOS

ANEXO I – SELEÇÃO DAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO UTILIZADAS NO CONTEXO BANCÁRIO (DINIZ, 2004):

Certificados digitais: utilizados para autenticar o usuário e o sistema.

Dispositivos one-time (token): utilizados como fator de autenticação, este tipo de dispositivos faz uso de senhas que podem ser utilizadas apenas por uma vez.

Cartões one-time: Trata-se de uma senha disponível apenas para uma transação. –

Proteção do navegador: proteção contra programas maliciosos.

Teclados virtuais: dispositivos baseados em criptografia que permitem a digitação de senha mais segura.

Dispositivos registrados: método que restringe o acesso ao sistema bancário apenas aos dispositivos registrados pelo banco. Esse tipo de técnica é considerado pelos especialistas de "impressão digital de hardware" e é aplicada em conjunto com mecanismos de identificação de usuários.

CAPTCHA - Completely Automated Public Turing test to tell Computers Humans Apart **:** trata-se de um método para fazer diferenciação entre computadores e seres humanos, cujo objetivo é proteger o sistema de ataques automatizados. As *CAPTCHA*s mais conhecidas são as imagens distorcidas de um código alfanumérico, de difícil reconhecimento por robôs automatizados (bots), onde o usuário deve introduzir num campo o reconhecimento desse código.

SMS - Short Message Service: Além de ser uma ferramenta para relacionamento com clientes. O SMS serve como mecanismo de segurança, sendo caracterizado como segundo canal de autenticação para determinadas transações por meio de um

conjunto de caracteres enviados ao usuário a fim de autorizar e processar através do sistema bancário online.

Identificação Positiva: é um modelo de autenticação, complementar às credenciais tradicionais de segurança (senha e código de acesso). Onde o sistema requer do usuário uma resposta correta de perguntas aleatórias, cujas respostas são extraídas das informações cadastrais do cliente. Trata-se de mais um método de autenticação secundária.

Monitoramento de transação: trata-se da análise do histórico de transações para identificar distorções no padrão de transações processadas.

Passphrase ou Palavra de passe: é um mecanismo de autenticação secundário, onde a senha é uma seqüência de caracteres maiores que a senha habitual (que é normalmente de 4 a 16 caracteres).