UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

ESCOLA DE ADMINISTRAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

KARL HEINZ BENZ

ALINHAMENTO ESTRATÉGICO ENTRE AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E AS ESTRATÉGIAS E PRÁTICAS ADOTADAS NA TI: ESTUDOS DE CASO EM INSTITUIÇÕES FINANCEIRAS

Porto Alegre

2008

KARL HEINZ BENZ

ALINHAMENTO ESTRATÉGICO ENTRE AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E AS ESTRATÉGIAS E PRÁTICAS ADOTADAS NA TI: ESTUDOS DE CASO EM INSTITUIÇÕES FINANCEIRAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial da obtenção do título de Mestre em Administração.

Orientadora: Profa. Dra. Ângela F. Brodbeck

Porto Alegre

2008

Dados Internacionais de Catalogação na Publicação (CIP)

B479a Benz, Karl Heinz.

Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI : estudos de caso em instituições financeiras / Karl Heinz Benz. – 2008.

200 f. ; il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul, Escola de Administração, Programa de Pós-graduação em Administração, 2008.
Orientadora: Profa. Dra. Ângela Freitag Brodbeck.

1. Tecnologia da informação. 2. Sistemas de informação. 3. Segurança da informação – Políticas. 4. Planejamento estratégico. 5. Alinhamento estratégico. I. Título.

Ficha elaborada pela Biblioteca da Escola de Administração – UFRGS

À minha esposa, Carmen,
e ao meu filho, Pedro,
pelo grande apoio que me deram
nos tantos momentos em que
as muitas dificuldades que enfrentei
na execução desta tarefa
quase me derrubaram.

Ao meu pai, Eberardo,
pela sua infinita capacidade de luta,
que acabou me contagiando
de alguma maneira.

À minha mãe, Myriam, in memoriam.

.

AGRADECIMENTOS

Deixo nesta página uma homenagem a todos aqueles que, de alguma forma, contribuíram no desenvolvimento da presente dissertação.

À minha orientadora, Profa. Dra. Ângela Freitag Brodbeck, pela orientação segura, e pela paciência.

Aos professores Dr. Antonio C. G. Maçada, Dr. Eduardo R. Santos, Dr. Henrique Freitas, Dr. João L. Becker, e Dr. Norberto Hoppen, pelos conhecimentos passados nas disciplinas e pelas discussões, sempre presentes, e à Profa. Dra. Denise Lindstrom Bandeira.

A todos os colegas da turma de Mestrado 2006, pelo companheirismo; aos colegas do Doutorado com quem tive mais contato, especialmente a Maria Amélia e o André.

Aos colegas de serviço, que de alguma forma me incentivaram e apoiaram: Aline, Antonio, Frédi, Ionara, Marco, Marisa, Motta, e Simone.

Ao Luís Carlos Janssen, pelas tantas colaborações.

Às empresas onde realizei as entrevistas, e às pessoas entrevistadas, que não cito para manter o sigilo solicitado.

RESUMO

A crescente importância da TI nas organizações torna crucial o alinhamento estratégico da política de segurança da informação, definida pelas organizações em função de normas locais e nacionais, regulamentos e melhores práticas, com as estratégias de TI específicas para segurança da informação, definidas no Planejamento Estratégico de Sistemas de Informação (projetos e práticas implementadas de Segurança da Informação). Caso contrário, facilmente os resultados do planejamento de TI poderão ser comprometidos por problemas de segurança. Assim, analisar o alinhamento da política de segurança com o planejamento de TI passa a ser muito importante para o bom desempenho da organização.

O objetivo desta Dissertação de Mestrado foi identificar as principais características encontradas nos modelos de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, assim como os principais fatores habilitadores e inibidores do mesmo, em organizações da área financeira com atuação no Rio Grande do Sul. Para atingir este objetivo foram realizados Estudos de Caso descritivos e exploratórios em três instituições financeiras: um banco comercial de economia mista, um banco comercial cooperativado e uma instituição financeira pública de fomento. Este último utilizado como caso de contraste. Para tanto foram entrevistados um total de 13 profissionais representativos ao teor desta pesquisa.

Ao final deste estudo é gerada uma lista de fatores habilitadores (apoio ativo da Diretoria; criação de estrutura específica de Segurança da Informação, posicionada hierarquicamente no mesmo nível que a TI; Política de Segurança da Informação configurada em 3 (três) níveis: estratégico, tático e operacional; ameaça do impacto de uma quebra na segurança; conformidade com leis, regulamentações específicas, padrões relevantes, contratos e diretrizes estratégicas corporativas; aderência a padrões de TI, como COBIT e ITIL, e segurança da informação, como a norma ABNT ISO 17799:2005; efeitos da estratégia sobre a TI e segurança da informação; ferramentas de TI como ferramentas estratégicas; existência de políticas de segurança específicas; controles e procedimentos de segurança incorporados aos sistemas; participação da segurança da informação no ciclo de vida dos sistemas; projetos de TI como ameaça; consciência da segurança da informação por parte dos usuários internos; normas de relacionamento com usuários; critérios de aceitação de sistemas; controles e procedimentos de prevenção, detecção e recuperação contra incidentes de segurança; confiabilidade, segurança e estabilidade da infra-estrutura) e inibidores (pouca importância

para a Segurança da Informação, com seu posicionamento hierárquico subordinado à TI; ausência de Política de Segurança da Informação formalizada em 3 níveis; falta de conformidade; efeitos negativos não detectados de novas estratégias corporativas na TI e na segurança da informação; a segurança da informação não fazendo parte do ciclo de vida dos sistemas; ameaças não detectadas de projetos de TI à segurança da informação; falta de consciência do uso seguro dos sistemas por parte dos usuários internos; falta de consciência do uso seguro dos sistemas por parte dos clientes).

Por fim, uma das principais implicações práticas deste estudo foi confirmar o uso da norma ABNT ISO 17799:2005 como padrão para a implantação de políticas de segurança da informação nas instituições financeiras com atuação no Rio Grande do Sul. Como principal contribuição acadêmica pode-se dizer que esta dissertação vem somar-se a alguns poucos trabalhos acadêmicos, tais como Oliva (2003) e Lessa (2006), no sentido de refletir sobre o alinhamento estratégico da segurança da informação.

Palavras-chave: alinhamento estratégico, segurança da informação, ISO 17799, tecnologia da informação.

ABSTRACT

The growing importance of IT in organizations makes crucial the strategic alignment of the policy of information security, defined by the organizations on the basis of local and national standards, regulations and best practices, with the specific strategies of IT to the information security, defined in the Strategic Planning of Information Systems.

Otherwise, easily the results of the planning of IT may be compromised by security problems. So the examine of the alignment of security policy with planning IT becomes very important to the performance of the organization.

The goal of this dissertation was to identify the main features found in models of strategic alignment between the policies of information security and the strategies and practices adopted in the IT, as the main enablers and inhibitors factors of this alignment, in financial organizations in Rio Grande do Sul.

To achieve this goal, Case Studies were performed descriptive and exploratory in three financial institutions: a commercial bank of mixed economy, a cooperative commercial bank and a public financial institution, the latter used as a case of contrast. There were interviewed a total of 13 highly professional representative to the content of this research.

At the end of this study there are generated hypotheses about the strategic alignment in question, and a list of factors enablers and inhibitors.

Finally, a major practical implications of this study was to confirm the use of the standard ABNT ISO 17799:2005 as standard for the implementation of policies of information security at financial institutions in Rio Grande do Sul.

The main academic contribution can be said that this dissertation is to add a few scholarly works, such as Oliva (2003) and Lessa (2006), to reflect on the strategic alignment of the security of information.

Key-words: strategic alignment, information security, ISO 17799, information technology.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AE	Alinhamento estratégico
ATM	*Automated Teller Machine*
BACEN	Banco Central do Brasil
BIS	*Bank for International Settlements*
CCSC	*Commercial Computer Security Centre*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
COBIT	*Control Objectives for Information and related Technology*
CSI/FBI	*Computer Security Institute/Federal Bureau of Investigations*
CVM	Comissão de Valores Mobiliários
FEBRABAN	Federação Brasileira de Bancos
FGV/EAESP	Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas
FISMA	*Federal Information Security Management Act*
IBM	*International Business Machines*
IEC	*International Electrotechnical Commission*
ISO	*International Standards Organization*
IT	*Information Technology* (TI)
ITIL	*Information Technology Infrastructure Library*
ITGI	*IT Governance Institute*
NIST	*National Institute of Standards and Technology, U. S. Department of Commerce*
OGC	*The United Kingdom's Office of Government Commerce*
PESI	Planejamento Estratégico de Sistemas de Informação

PETI	Planejamento Estratégico de TI
TI	Tecnologia da Informação
TISS	Troca de Informações em Saúde Suplementar
UK DTI	*United Kingdom - Department of Trade Center*

SUMÁRIO

1 INTRODUÇÃO

Os investimentos em TI não resultavam em agregação de valor, o que seria em parte devido à falta de alinhamento entre as estratégias de negócios e as estratégias de TI nas organizações, conforme afirmação feita em um artigo publicado por Henderson e Venkatraman (1993). Muitos estudos se seguiram, com alguns autores complementando as definições iniciais, e outros tecendo críticas aos conceitos ou à forma tomada para algumas das implementações nas organizações e os resultados efetivos obtidos. Brodbeck e Hoppen (2003), em pesquisa na qual buscam estender o modelo inicial de Henderson e Venkatraman (1993), observam que "*o foco do alinhamento estratégico entre o negócio e a TI deve se concentrar na promoção de alinhamento contínuo para todo o horizonte de planejamento, evidenciando a persistência do processo no ciclo de vida da organização*".

Alinhamento estratégico é um tema que não se restringe ao meio acadêmico. Documento conjunto do *The IT Governance Institute* (responsável pelo COBIT – padrão de auditoria) e do *The Office of Government Commerce* (responsável pelo ITIL – padrão de governança de TI) diz claramente que "como a governança de TI – tanto o conceito quanto a prática efetiva – vem ganhando oportunidade e aceitação, as melhores práticas de TI serão cada vez mais alinhadas ao negócio e aos requisitos da governança, ao invés de se preocuparem apenas com requisitos técnicos" (ITGI, 2005).

- Esta dissertação buscou abordar a questão do alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas pela TI, visando que esta agregue maior valor ao negócio. O que se busca nesta dissertação, restringindo a amplitude do tema, é descobrir quais são os fatores habilitadores e inibidores da promoção do alinhamento estratégico das políticas de segurança de

informação nos níveis estratégico, tático e operacional, em instituições bancárias com atuação no Rio Grande do Sul.

A questão do alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI se torna relevante em função dos grandes investimentos que as organizações fazem nesta área, dos muitos riscos relacionados à segurança e da falta de sincronia entre administração das organizações e segurança da informação. Neste sentido, esta idéia pode ser assegurada pelo depoimento de Balbo (2007):

> É muito comum encontrar um cenário onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional e definido pela análise de risco.

Assim, não é difícil perceber o mesmo sintoma que Henderson e Venkatraman (1993) detectaram em relação à TI: os investimentos em segurança da informação por vezes não resultam em agregação de valor.

Por outro lado, a norma brasileira da ABNT que versa sobre segurança da informação, a NBR ISO 17799:2005, tradução literal da ISO/IEC 17799, em uma visão voltada para o negócio, trata a informação como de seus mais importantes ativos ao conceituá-la como:

> Informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. [...] A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas (ABNT, 2005).

Esta necessidade da proteção da informação se prende ao fato de que “a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa” (SÊMOLA, 2003). Sendo assim, toda a estratégia de segurança da informação deve buscar um alinhamento permanente aos objetivos estratégicos definidos pela organização. Com isto, é possível suportar e sustentar sua

estratégia competitiva, proteger seus ativos críticos, minimizar riscos, e controlar o ambiente organizacional (OLIVA, 2003).

Por isso é tão importante para os negócios ficar atento aos fatores habilitadores e inibidores de um alinhamento estratégico entre as políticas e estratégias de segurança das informações e as práticas adotadas efetivamente pela TI, tão obrigatórias para determinadas organizações, como bancos, empresas de saúde, etc. Dentre os principais fatores habilitadores deste tipo de alinhamento, encontram-se o apoio e comprometimento da alta administração (PELTIER, 2002; ABNT, 2005; VON SOLMS, 2006; LESSA, 2006); a presença de estruturas organizacionais específicas (ABNT, 2005; VON SOLMS, 2006); a política de segurança da informação, objetivos e atividades que reflitam os objetivos do negócio (ABNT, 2005); a divulgação/conscientização eficiente da segurança da informação para todos os funcionários (OLIVA, 2003; ABNT, 2005); o estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação (ABNT, 2005); e a conformidade com leis e regulamentos (ABNT, 2005; VON SOLMS, 2006). Da mesma forma, estes mesmos estudos apontam como principais fatores inibidores deste tipo de alinhamento a falta de apoio visível da diretoria (PELTIER, 2002); a divulgação ineficaz da segurança junto aos funcionários e/ou treinamento inadequado (PELTIER, 2002); e a falta de um programa de medição da eficácia do controle (PELTIER, 2002).

Em decorrência da sua importância crescente, a segurança da informação está sendo alvo de normatização. A norma mundial mais relevante do setor é a ISO/IEC 17799, que foi traduzida pela ABNT (Associação Brasileira de Normas Técnicas), tendo recebido a denominação de ABNT NBR ISO/IEC 17799:2005 (ABNT, 2005). Também é relevante a extensa série de documentos relativos à segurança editados pelo NIST – *National Institute of Standards and Technology, U. S. Department of Commerce,* embasado no *"Federal*

Information Security Management Act" (FISMA), que determina a adoção de padrões básicos de segurança para todos os sistemas do governo americano (FISMA, 2004). Padrões (*frameworks*) de governança, como COBIT - *Control Objectives for Information and Related Technology* (ITGI, 2006) e ITIL - *Information Technology Infrastructure Library* (ITIL, 2006) - igualmente têm sessões que tratam especificamente da segurança da informação.

Por outro lado, crescentes regulamentações governamentais, em nível mundial, como a lei americana Sarbanes-Oxley e o chamado "Acordo da Basiléia", vêm exigindo que as organizações encarem a informação com mais seriedade, o que implica necessariamente uma segurança da informação mais rigorosa e mais voltada para o negócio. No caso específico do setor financeiro brasileiro, objeto de estudo desta dissertação, existe uma regulamentação governamental (Apêndice A), que tende a seguir o modelo do "Acordo da Basiléia", materializada principalmente em algumas resoluções do BACEN (Banco Central do Brasil), principalmente a Resolução 2.554 (Controles Internos) e a Resolução 3.380 (Risco Operacional), que qualifica como um dos riscos operacionais a serem mitigados as falhas em sistemas de tecnologia da informação (CARNEIRO ET AL., 2005).

1.1 JUSTIFICATIVA

Incidentes na área de segurança da informação podem ter conseqüências catastróficas nas organizações, pois podem afetar a estratégia competitiva com a quebra de credibilidade, vazamento de informações estratégicas e possível geração de imagem negativa da organização no mercado (OLIVA, 2003). E isto vale especificamente na área bancária no Brasil, conforme cita Márcio Cypriano, presidente da Febraban (Federação Brasileira de Bancos), que observa que os investimentos em novas tecnologias e infra-estrutura chegaram a cerca de R$ 5,3 bilhões em 2006, dos quais um total de 8 a 10% foram investidos em novas ferramentas e sistemas de segurança (COMPUTERWORLD, 2006).

Recente pesquisa realizada pela FGV/EAESP mostra que “as empresas atribuem maior importância aos aspectos de privacidade e segurança, alinhamento estratégico, adequação organizacional e tecnológica, e relacionamento com clientes” (ALBERTIN, 2005). Isto também pode ser observado pelas considerações da Sra. Zilta Marinho, diretora da empresa Módulo, quando afirma que “na sociedade do conhecimento o principal patrimônio é a informação, e para o sucesso e a continuidade do negócio ela deve ser protegida.” (MÓDULO, 2005). Complementando, Sêmola (2003) explica que a informação precisa ser protegida por diversos motivos: pelo seu valor, pelo impacto de sua ausência, pelo impacto resultante de seu uso por terceiros, pela importância de sua existência, pela relação de dependência com a sua atividade.

Por sua vez, a norma ISO/IEC 17799:2005 – “Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação” – ressalta que a informação é importante ativo da organização, e que a confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o

faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado. Além disso, a dependência cada vez maior da organização em relação aos seus sistemas de informação revela uma vulnerabilidade considerável (ABNT, 2005).

No entanto, a segurança da informação parece não ser assunto da alta administração das organizações. Como ressaltavam Straub e Welk (1998),

> "A segurança da informação continua a ser ignorada pela alta administração, gerentes intermediários, e funcionários em geral. O resultado desta negligência é que os sistemas organizacionais são muito menos seguros do que poderiam ser e as brechas de segurança são mais freqüentes e causam mais danos do que o necessário".

Praticamente uma década depois, a situação parece não ter mudado, pois

> "É muito comum encontrar um cenário onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional e definido pela análise de risco (BALBO, 2007)".

Não é difícil perceber que o mesmo sintoma que Henderson e Venkatraman (1993) detectaram em relação à TI, de que os investimentos em segurança da informação por vezes não resultavam em agregação de valor, possivelmente esteja se repetindo em relação à segurança da informação.

No entanto, os principais resultados da pesquisa (*survey*) realizada por Oliva (2003), sobre a importância da Política de Segurança da Informação de acordo com a norma ABNT ISO 17799:2005 na estratégia competitiva, indicam que as empresas percebem que a política de segurança da informação suporta a estratégia competitiva e que um incidente de segurança pode causar impacto na competitividade da organização no mercado.

Num setor da economia, como o bancário, onde se verifica a presença de regulamentação governamental (principalmente a Resolução 3.380 do BACEN), a segurança da informação assume um papel crítico na condução do negócio.

1.2 QUESTÃO DE PESQUISA

Dada à importância e relevância atual do tema e a necessidade de se encontrar modelos que demonstrem ou expliquem o alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, assim como evidenciar os fatores que podem inibir ou melhorar a promoção deste alinhamento, foi identificada a seguinte questão de pesquisa:

- Como está sendo realizado o alinhamento estratégico entre as políticas da segurança da informação requeridas pelo negócio (normas e regulamentações) e as estratégias e práticas de segurança de informação adotadas pela TI?

1.3 OBJETIVOS

O objetivo principal desta pesquisa foi analisar as características da promoção do alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI para os níveis estratégico, tático e operacional, bem como os fatores habilitadores e inibidores deste alinhamento, em instituições financeiras com atuação no Rio Grande do Sul.

No intuito de atingir o objetivo principal, são propostos os seguintes objetivos específicos:

- Identificar, na literatura, os principais fatores habilitadores e inibidores de alinhamento estratégico entre as políticas de segurança de informação de negócios e as estratégias e práticas implementadas pela TI para suportar tal necessidade;

- Identificar as principais políticas, normas e resoluções de segurança de informação praticadas nas instituições financeiras pesquisadas com atuação no Rio Grande do Sul; e

- Listar os principais fatores habilitadores e inibidores atuantes nas instituições financeiras pesquisadas.

1.4. ESTRUTURA DESTE DOCUMENTO

Este documento apresenta as seguintes seções: introdução, referencial teórico, metodologia, estudos de caso, análise dos resultados e conclusões.

O capítulo 1 é a introdução, que contém conceitos básicos sobre o tema em estudo, sua relevância, a atualidade e a justificativa, os quais levaram às questões de pesquisa. No intuito de responder estas questões, foram propostos o objetivo principal e 4 objetivos específicos.

O estudo será desenvolvido a partir deste arcabouço, no qual se esboça uma visão geral do trabalho. O presente capítulo contextualiza o tema, define o problema de pesquisa e os objetivos (principais e específicos) e apresenta a justificativa para a escolha do tema.

O Capítulo 2 é dedicado às referências teóricas, abordando três grandes temas: alinhamento estratégico (incluindo definição e modelos, e fatores habilitadores e inibidores), tecnologia da informação (incluindo sistemas de informação, planejamento estratégico de TI, e governança de TI), e segurança da informação (incluindo um breve histórico, a norma ABNT ISO 17799:2005, críticas à norma e às políticas de segurança, segurança e sistemas de informação, segurança da informação e governança, e fatores habilitadores e inibidores do alinhamento estratégico). O capítulo prossegue com as regulamentações governamentais (do setor financeiro no Brasil) e termina por mostrar o Modelo Preliminar para Estudo e as dimensões, elementos e variáveis de pesquisa.

O Capítulo 3 apresenta o método utilizado nesta pesquisa explicitando o processo da coleta de dados nos casos estudados, a forma de análise dos dados e tece considerações sobre a validade e a confiabilidade da pesquisa.

O Capítulo 4 apresenta os resultados da pesquisa realizada nos 3 Estudos de Caso, considerando as dimensões, os elementos e as variáveis de pesquisa.

O Capítulo 5 mostra a análise efetuada, que possibilitou o entendimento dos dados coletados, e termina com a contraposição dos resultados com o Modelo Preliminar para Estudo.

O Capítulo 6 apresenta as conclusões desta dissertação, apresentando as limitações da pesquisa, as contribuições e as pesquisas futuras.

2 REFERENCIAL TEÓRICO

O presente capítulo aborda três grandes temas: Alinhamento Estratégico (incluindo definição e modelos, e fatores habilitadores e inibidores), Tecnologia da Informação (incluindo sistemas de informação, planejamento estratégico de TI, e governança de TI), e Segurança da Informação (incluindo um breve histórico, a norma ISO/IEC 17799, críticas à norma e às políticas de segurança, segurança e sistemas de informação, segurança da informação e governança, e fatores habilitadores e inibidores do alinhamento estratégico). A seguir, o capítulo aborda as definições específicas do setor financeiro no Brasil (regulamentações governamentais, definição de instituição financeira, marco regulatório da área financeira, os "Acordos da Basiléia", e iniciativas legais que afetam a segurança da informação).

2.1 ALINHAMENTO ESTRATÉGICO

O alinhamento estratégico (AE) diz respeito ao alinhamento dos recursos organizacionais com as ameaças e as oportunidades do ambiente. As estratégias de negócio devem refletir as decisões que, alinhadas aos recursos corporativos, entre os quais se inclui a TI, ajudam a ligar as organizações com seu ambiente. Especificamente, em relação à TI,

> os modelos atuais focam o AE como um processo contínuo e constante durante a etapa da implementação do Planejamento Estratégico. [...] Eles buscam observar as melhores práticas de promoção do AE, o seu nível de maturidade, as práticas habilitadoras/inibidoras e o grau de importância da promoção do alinhamento para cada elemento (BRODBECK ET AL., 2003).

À medida que a tecnologia da informação foi se tornando mais importante, começou a ser discutido seu verdadeiro papel em relação ao negócio das organizações, pois a TI era vista

como algo distinto e separado do negócio, cumprindo algumas funções específicas, mas sem vínculo com a estratégia organizacional.

2.1.1 Definição

No início da década de 1990, Henderson e Venkatraman (1993) observaram que os investimentos em TI não resultavam em agregação de valor, o que seria devido, em parte, à falta de alinhamento entre as estratégias de negócios e as estratégias de TI nas organizações. Segundo os autores, a estratégia envolveria a formulação (decisões que dizem respeito à competitividade e às escolhas de produtos e mercados) e a implementação (escolhas relativas à estrutura e capacidades da organização para executar e dar suporte às suas escolhas de produtos e mercados).

O alinhamento estratégico, para Henderson e Venkatraman (1993), não é um evento isolado, mas um processo contínuo de adaptação e mudança, no qual as vantagens competitivas desejadas são obtidas através da capacidade de uma organização de explorar continuadamente a sua funcionalidade de TI.

Em suma, o conceito de alinhamento estratégico, conforme Henderson e Venkatraman (1993), pode ser visto como adequação estratégica e integração funcional entre as estratégias de negócio e as estratégias de TI. A adequação estratégica reconhece a necessidade de que cada estratégia faça referência aos domínios externo (ambiente de negócios, onde as firmas competem e tomam decisões relativas à oferta de produtos aos mercados, aquisição ou confecção própria de determinado produto, parcerias, alianças) e interno (escolhas referentes à estrutura administrativa, organização funcional, processos críticos e recursos humanos).

O modelo de Henderson e Venkatraman serviu como base para diversos autores. Luftman, Lewis e Oldach (1993) defendem que o alinhamento estratégico reflete a visão de que o sucesso dos negócios depende da harmonia entre quatro fatores: a estratégia de negócio, a estratégia da TI, a infra-estrutura organizacional e de processos, e a infra-estrutura de TI e de processos. Para os autores, a falta de sincronia entre negócios e TI criou muita tensão dentro das organizações, resultando em perda de retorno sobre o investimento em TI.

Alinhamento de curto e longo prazos são definidos por Reich e Benbasat (1996). O alinhamento de curto prazo seria um processo no qual executivos de negócio e executivos de TI comprometem-se uns com os outros e com os planos e objetivos de curto prazo (1-2 anos), ao passo que o alinhamento de longo prazo seria um processo no qual executivos de negócios e de TI compartilham uma visão de futuro (3-5 anos), na qual a tecnologia da informação contribui para o sucesso do negócio.

Claudio Ciborra (1997) relata que em 1991 foi lançado o conceito de TI como um elo variável entre estratégia, organização e cultura. Em 1993, no IBM Systems Journal, Henderson e Venkatraman lançaram o conceito de alinhamento estratégico. A partir daí, segundo Ciborra, começam a se estabelecer dificuldades conceituais: como avaliar se uma empresa está alinhada, e como medir o alinhamento? Em 1995 a IBM cortou o financiamento dos projetos relativos ao assunto, e em 1996 Broadbent, Weill, O'Brien e Neo publicaram artigo abordando a "ligação" entre a estratégia e a TI, sem referenciar o termo "alinhamento estratégico". Ciborra (1997) questiona o conceito de alinhamento estratégico nos negócios. Diz que enquanto o alinhamento estratégico é considerado como verdade absoluta e incontestável, no mundo real ele está longe de ser implementado. O autor chega a dizer que o alinhamento estratégico é como a ponte que um dia ligará a Sicília à Itália: vive sendo reprojetada e não sai nunca do papel, além de ser sujeita a diversos tipos de terremotos.

Entre as muitas críticas de Ciborra (1997) ao alinhamento estratégico, podem ser citadas:

- Há diversas características na infra-estrutura de TI que impedem o seu alinhamento estratégico;

- Sugere que o alinhamento estratégico, da forma como é proposto, é uma “aliança estratégica entre humanos e não-humanos”;

- Alinhamento estratégico fala em “fenômenos que ocorrem naturalmente”, mas mede construtos teóricos e artificiais;

- Apóia-se num estilo de ensino, pesquisa e consultoria que envenena as práticas e pensamento gerenciais com modelos simplificados que têm um ciclo de vida curto;

- Não considera o aspecto das pessoas: “A existência humana, cuidadosamente desconsiderada nos modelos, espera-os (os adeptos do alinhamento estratégico) em seus locais de trabalho”;

- Os detalhes conceituais permanecem no mundo das abstrações, com pouco impacto nas organizações.

Ciborra (1997) sugere um caminho alternativo: voltar às evidências básicas, e enxergar o mundo como ele realmente é. De qualquer maneira, a “ponte que liga a Sicília à Itália” precisa ser construída, ou seja, a TI precisa estar alinhada à estratégia das organizações, visando dar melhores condições para o crescimento do negócio e a vantagem competitiva.

O desalinhamento entre planejamento de TI e planejamento da organização ocorre quando estes dois planejamentos estão em direções diferentes, com baixa interação e comunicação insuficiente entre eles. O alinhamento estratégico é um processo evolucionário e dinâmico, que requer forte apoio da alta gestão das organizações, associado a boas relações de trabalho, liderança forte, priorização adequada, confiança e efetiva comunicação, além do correto entendimento do ambiente de negócios (LUFTMAN, 2000).

O entendimento de alinhamento estratégico é ampliado para além do aspecto conceitual, sendo tratado como uma ferramenta de monitoramento e gestão das estratégias e objetivos da organização. Devido à rapidez das mudanças no ambiente de negócios, as estratégias e objetivos podem passar por ajustes e reorientações, o que irá levar a um processo de alinhamento constante (BRODBECK, 2001).

O modelo original de Henderson e Venkatraman, de 1993, é estendido por Brodbeck e Hoppen (2003),

> "abrindo-o para a etapa de implementação do processo de planejamento e fornecendo elementos para a sua implementação. O foco do modelo passa a ser a promoção de alinhamento contínuo para todo o horizonte de planejamento, evidenciando a persistência do processo no ciclo de vida da organização. A dimensão alinhamento é tratada independentemente da dimensão planejamento estratégico, evidenciando a sua importância como processo único e não mais isolado para a área de negócios ou para a área de TI. A visão passa a ser de gerenciamento das estratégias do negócio, tendo a tecnologia como um recurso obrigatório para o sucesso dos negócios."

2.1.2 Fatores Habilitadores e Inibidores

Os fatores habilitadores são os que facilitam o alinhamento; os fatores inibidores são os que dificultam o alinhamento estratégico entre negócio e TI. A ausência de um certo fator

habilitador não implica, necessariamente, que este mesmo fator passe a funcionar como inibidor, como é deixado implícito por Luftman, Papp e Brier (1999).

Em pesquisa longitudinal com duração de cinco anos (1992 a 1997), Luftman, Papp e Brier (1999) encontraram fatores organizacionais consistentes cuja presença ou forte atenção exercia papel promotor, mas cuja ausência ou fraca atenção exercia papel inibidor do alinhamento estratégico da estratégia de TI com a estratégia empresarial. O estudo foi baseado na falta de resultados consistentes nos estudos iniciais de alinhamento estratégico.

Os principais fatores habilitadores detectados no estudo foram:

- Apoio da alta gestão aos assuntos de TI;
- Envolvimento da TI no desenvolvimento da estratégia;
- Compreensão do negócio por parte da TI;
- Parceria entre TI e área de negócios;
- Projetos de TI corretamente priorizados;
- TI demonstrando liderança.

O mesmo estudo de Luftman, Papp e Brier (1999) aponta os elementos inibidores do alinhamento estratégico entre negócio e TI:

- Falta de relacionamento estreito entre TI e área de negócios;
- TI mal priorizada;

- Falha da TI em cumprir seus compromissos;
- Falta de compreensão dos negócios por parte da TI;
- Falta de suporte à TI por parte dos altos executivos;
- Lapso de liderança da gerência de TI.

Duas etapas são consideradas por Brodbeck et al. (2003) para o alinhamento estratégico (formulação e implementação); a etapa de formulação teria como elementos para promoção do alinhamento: adequação estratégica entre os componentes de negócio e de TI; integração funcional através da representação do modelo de negócio nos sistemas de informação integrados; e integração informacional (consistência entre os objetivos planejados e as informações dos sistemas de informação para suporte ao monitoramento dos mesmos durante a sua execução). Para a etapa de implementação, além da presença dos três elementos anteriores, os autores adicionaram mais quatro elementos promotores de alinhamento: metodologia de implementação (para dar impulso à adequação contínua dos itens planejados na etapa anterior); comprometimento das pessoas com a obtenção das metas; sincronização dos recursos entre as ações de negócio e de TI; e instrumentação de gestão, pelo uso de ferramental adequado, que permita a integração funcional e informacional para o eficiente monitoramento e ajuste contínuo dos processos, objetivos e metas planejadas.

Haveria ainda, neste mesmo modelo, dois elementos promotores: um contexto organizacional que propicie uma cultura de gestão corporativa, postura decisória pró-ativa, política de incentivos e representatividade do modelo de negócios nos sistemas de informação integrados, e um modelo de planejamento estratégico com um maior grau de formalismo com

relação aos componentes do plano estratégico de negócio e planejamento estratégico de TI (BRODBECK ET AL., 2003).

Os principais fatores habilitadores e inibidores do alinhamento estratégico entre a estratégia de TI e a estratégia empresarial levantados na literatura são (PEREIRA, 2006):

- Fatores habilitadores: apoio da alta gestão, participação, entendimento do negócio, parceria, prioridade, liderança, comunicação clara, compartilhamento, conexão, comprometimento, sincronização, monitoramento, e postura pró-ativa.

- Fatores inibidores: relações fracas, falta de Prioridade, falha no comprometimento, falha de entendimento do negócio, falta de apoio da alta gestão, fraca liderança, falta de participação, falta de conhecimento, falha na implementação, inabilidade para mudanças, dificuldade na gestão, e dificuldade de monitoramento.

2.2 TECNOLOGIA DA INFORMAÇÃO

A tecnologia da informação, componente vital na atual configuração competitiva e produtiva das organizações, tem assumido importância crescente nas organizações, principalmente a partir do início dos anos 80. Até o fim dos anos 70, o processamento de dados era usado como meio de reduzir os custos dos processos administrativos. De início, o uso dos computadores na operação dos negócios organizacionais visava à eficiência, a racionalização do processo operacional e uma forma mais produtiva de explorar os recursos.

Rapidamente, a TI foi tendo seu uso disseminado nas organizações, gerando benefícios em termos de eficiência, eficácia e transformação. Para Laudon e Laudon (2004), a tecnologia da informação é a infra-estrutura que permite armazenar, buscar, recuperar, copiar, filtrar, manipular, visualizar, transmitir e receber informação. Luftman, Lewis e Oldach (1993), já abordando a questão sob o ponto de vista do alinhamento estratégico, consideram que a TI proporciona valor estratégico para todas as partes do negócio e, embora ainda seja usada para reduzir custos, seu atual foco é alavancar produtos e serviços de qualidade, melhorar serviço e operações de clientes, integrar fornecedores e tornar possível a aprendizagem organizacional. Na visão dos autores, o uso estratégico da tecnologia da informação produz um impacto poderoso no negócio e amplia o valor da informação (PEREIRA, 2006).

2.2.1 Sistemas de Informação

Os sistemas de informação, na opinião de O'Brien (2001), são desenvolvidos para suprir necessidades específicas de cada nível de administração (suporte de processos e operações, suporte na tomada de decisões e suporte na implantação da estratégia competitiva). Há diversas classificações de sistemas; conforme Perottoni et al. (2001), os tipos de sistemas de informações e seus relacionamentos são:

- SIT (Sistema de Informação Transacional ou Sistema de Processamento de Transações): monitoram, coletam, armazenam, processam e distribuem os dados das diversas transações realizadas dentro da empresa, servindo como base para os demais sistemas corporativos;

- SIG (Sistema de Informação Gerencial): agrupa os dados disponibilizados no SIT e coleta, valida, executa operações, transforma, armazena e apresenta informações para o uso do planejamento e orçamento, entre outras situações gerenciais;

- SAE (Sistema de Automação de Escritório): foca no processamento das informações de escritório, como processadores de textos, agendas eletrônicas, editores de imagens e a possibilidade de gerenciamento de diversos tipos de projetos, entre outros;

- SAD (Sistema de Apoio à Decisão): apóia decisões específicas sem substituir o julgamento humano, fornecendo suporte a decisões semi-estruturadas e não-estruturadas;

- DW e DM (*Data Warehouse* e *Data Mining*): *Data Warehouse* é um grande banco de dados contendo dados históricos resumidos em diversos níveis de detalhamento; *Data Mining* realiza inúmeras funções a partir do DW, como classificações, agrupamentos e estimativas;

- SE (Sistemas Especialistas): tratam de situações de decisão específicas (como, por exemplo, o diagnóstico médico);

- EIS (Sistemas de Informações para Executivos): realizam a filtragem dos dados mais relevantes para os executivos, a partir de bancos de dados do SIT, SIG e em fontes internas e externas, reduzindo o tempo de obtenção e gerando informações de real interesse, as quais permitam o acompanhamento e controle da organização;

- ERP (Sistema de Gestão Empresarial): administram partes importantes da empresa, tais como o planejamento do produto, compras de componentes, manutenção de estoques, interação com fornecedores, entre outros, fornecendo assim, informações importantes para os negócios *on-line*; englobam funções encontradas no SIT, SIG e EIS; o ERP integra em seus módulos todos os tipos de informação;

- CRM (*Customer Relationship Management*): tem foco no cliente, ou seja, visa administrar as informações sobre determinados clientes, fazendo com que a organização conheça seu comportamento e supere suas expectativas.

Ainda poderia ser acrescentado a esta classificação o SCM (*Supply Chain Management*), que realiza o gerenciamento da cadeia produtiva, desde o fornecimento da matéria-prima até a rede de distribuição dos produtos.

2.2.2 Planejamento Estratégico de TI

A literatura costuma usar os termos TI (tecnologia da informação) e SI (sistemas de informação); alguns autores consideram o termo “tecnologia da informação” mais amplo que “sistemas de informação”; outros, pelo contrário, consideram o termo “sistemas de informação” mais abrangente. Nesta dissertação os dois termos são considerados como sendo equivalentes; da mesma forma, são considerados equivalentes os termos PESI (Planejamento Estratégico de Sistemas de Informação) e PETI (Planejamento Estratégico de TI).

O Planejamento Estratégico de Sistemas de Informação (PESI) pode ser definido como o processo de identificação de um portfólio computadorizado de aplicações para dar

suporte ao plano de negócios da organização e auxiliar na concretização dos objetivos organizacionais. O PESI exerce um papel fundamental ao ajudar a “evitar oportunidades perdidas, esforços duplicados, sistemas incompatíveis e desperdício de recursos” (LEDERER e SETHI, 1988).

2.2.3 Governança de TI

A governança de TI “está diretamente relacionada com o objetivo de obter melhorias no desempenho da tecnologia no âmbito corporativo, envolvendo a adoção de uma série de guias para influenciar o comportamento empresarial e direcionar as atividades de TI” (STREIT ET AL., 2004 APUD MAÇADA ET AL., 2006). Visa responder à demanda dos acionistas por maior transparência e atender as exigências das novas legislações; também traz benefícios como excelência operacional, efetivo alinhamento entre TI e negócios e redução de custos (HARDY, 2006; CERIONI, 2004 APUD MAÇADA ET AL., 2006).

Como *framework* de governança de TI podem ser citados o COBIT – *Control Objectives for Information and Related Technology* (ITGI, 2006) e o *framework* de boas práticas de gestão de TI, o ITIL - *Information Technology Infrastructure Library* (OGC, 2007). Existe uma clara tendência na literatura (BERNARDES e MOREIRA, 2005) e no mercado (ITGI, 2005), no sentido de integrar estes *framewoks*, mais a ISO/IEC 17799 (no Brasil, ABNT ISO 17799:2005).

2.2.3.1 COBIT

O COBIT é um modo de implementar a governança de TI, desenvolvido pelo *IT Governance Institute* – ITGI (ITGI, 2003), criado em 1998 para definir padrões no direcionamento e controle da tecnologia da informação nas empresas. Uma governança de TI eficaz ajuda a garantir que a tecnologia da informação apóia efetivamente os objetivos de negócio, otimiza o investimento de TI e gerencia as oportunidades e ameaças relacionadas a TI.

Basicamente, o COBIT é um *framework* que deve ser customizado para cada empresa, devendo ser usado com outros recursos para personalizar as melhores práticas para o seu uso específico em cada empresa. O COBIT, na sua essência, possui quatro grandes grupos de gerenciamento e controle chamados domínios: PO - Planejamento e organização ("*Plan and organise*"); AI - Aquisição e implementação ("*Acquire and implement*"); DS - Entrega e suporte ("*Deliver and support*") e ME - Monitoração ("*Monitor and evaluate*").

Para estes domínios, existem 34 objetivos de controle, que por sua vez possuem *checklists* daquilo que é mais importante considerar em cada um.

2.2.3.2 ITIL

O ITIL (*IT Infrastructure Library*) é uma biblioteca composta pelas melhores práticas para gerenciamento de serviços de TI (ITIL, 2007). Criada pelo governo britânico em 1980, começou a tornar-se relevante no mercado no início dos anos 90. A biblioteca ITIL é composta por diversos livros, sendo os principais: Entrega de Serviços ("*Service Delivery*"),

Suporte a Serviços (“*Service Support*”), Gerenciamento da Segurança (“*Security Management*”), Gerenciamento da Infra-estrutura de TIC (“*ICT Infrastructure Management*”), Perspectiva do Negócio (“*The Business Perspective*”), Gerenciamento das Aplicações (“*Application Management*”), Gerenciamento de Recursos de Software (“*Software Asset Management*”).

O ITIL tem uma abordagem orientada a processos intimamente ligados, e integrados entre si. Esses processos estão divididos em dois grandes grupos, a saber:

- Gerenciamento de Serviços – Suporte; concentra-se na execução do dia-a-dia e no suporte a serviços de TI; engloba: *Service-Desk*, Gerenciamento de Configurações, Gerenciamento de Incidentes, Gerenciamento de Problemas, Gerenciamento de Mudanças, e Gerenciamento de Versões.

- Gerenciamento de Serviços – Entrega; concentra-se no planejamento e melhoria dos serviços de TI; engloba: Gerenciamento de Nível de Serviços, Gerenciamento de Capacidade, Gerenciamento Financeiro, Gerenciamento de Disponibilidade, e Gerenciamento de Continuidade.

2.3 SEGURANÇA DA INFORMAÇÃO

A NBR ISO/IEC 17799 define **informação** como sendo “um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida”. A mesma norma define **segurança da informação** como “a proteção da informação de vários 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" (ABNT, 2005).

2.3.1 Breve histórico da segurança da informação

Nos primeiros tempos da computação as aplicações eram basicamente militares, e os problemas de segurança eram restritos ao acesso físico (LANDWEHR, 2001).

Os primeiros problemas com segurança de computadores surgiram com a necessidade do compartilhamento do processamento de informações e recursos entre vários tipos de usuários, com níveis de confiança diferentes, o que levou ao desenvolvimento de sistemas operacionais de tempo compartilhado ("*time-sharing*"). Estes sistemas operacionais deveriam ser, idealmente, implementados de forma a garantir a segurança, mesmo considerando os problemas gerados pelo compartilhamento de recursos (terminais de acesso, dispositivos de armazenamento de dados com acesso aleatório, impressoras e os programas e sistemas). A partir desta nova realidade, o chamado "problema clássico" de segurança de computadores pode ser apresentado da seguinte forma: "Como fazer com que usuários autorizados possam ter acesso a determinadas informações, ao mesmo tempo em que os usuário não autorizados não possam acessá-las?" (NIST, 1996),

Em 1967 foi criado, nos Estados Unidos, com a contribuição de órgãos governamentais como o Departamento de Defesa (DoD) e a Agência Central de Inteligência (CIA), um documento intitulado "*Security Control for Computer System: Report of Defense Science Boad*", que representou o início do processo oficial de criação de um conjunto de regras para segurança de computadores (não se utilizava ainda a expressão "segurança da

informação"). Seguem-se outras iniciativas diversas, não somente nos Estados Unidos. Em outra iniciativa destinada a resolver o "problema clássico" de segurança, o Departamento de Defesa dos Estados Unidos formulou um plano que daria origem à "*DoD Computer Security Initiative*", que acabou redundando na criação de um conjunto de regras a serem utilizadas no processo de avaliação da segurança, conhecido informalmente como "*The Orange Book*", documento cuja versão final foi publicada apenas em 1985. A utilização do *Orange Book*, que estabelecia critérios para estipular níveis de segurança, facilitou a comparação de soluções fornecidas pela indústria, pelo mercado e pelo meio acadêmico de uma forma geral. Embora o padrão hoje seja considerado obsoleto, teve grande importância e deu origem a diversas documentações relativas à segurança da informação (GONÇALVES, 2004).

2.3.2 A Norma ABNT ISO 17799

O padrão mais aceito atualmente é a norma ISO/IEC 17799 - *Information Technology - Security Techniques - Code Of Practice For Information Security Management*. Esta ISO se originou de um esforço do governo britânico, que em 1987, através do UK DTI (*Departamente of Trade Center*) criou o CCSC (*Comercial Computer Security Centre*), cujo objetivo era a criação de critérios para a avaliação da segurança e de um código de segurança para os usuários das informações; sua primeira versão foi publicada em 1989, com o nome de "PD0003 - Código de Gerenciamento de Segurança da Informação". Submetido a diversas revisões e atualizações, o documento foi homologado pela ISO (*International Organization for Standardization*) em 2000, assumindo a denominação de ISO/IEC 17799:2000 (GONÇALVES, 2004). A norma foi mais uma vez atualizada, tendo sido gerada a ISO/IEC

17799:2005. Em julho de 2007 ela foi renomeada para ISO/IEC 27002 - *Information Technology - Security Techniques - Code Of Practice For Information Security Management*.

No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) houve por bem traduzir a norma literalmente, gerando a NBR ISO/IEC 17799 – "Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação" (ABNT, 2005).

A literatura já havia consagrado como objetivo da segurança da informação a preservação da confidencialidade, da integridade e da disponibilidade da informação; a norma NBR ISO/IEC 17799 amplia um pouco este escopo, estabelecendo como objetivo "*a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade ('accountability'), não-repúdio e confiabilidade, podem também estar envolvidas"* (ABNT, 2005).

A versão anterior da norma NBR ISO/IEC 17799 (ABNT, 2001) definia:

- Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

- Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A autenticidade é um pré-requisito para a confidencialidade, a integridade e a disponibilidade. O não-repúdio, também chamado de “irrefutabilidade”, ganha grande importância em transações legais ou financeiras, com vistas a evitar fraude (LANDWEHR, 2001).

Há controvérsias sobre a importância relativa entre os itens acima. Embora a norma ISO/IEC 17799 não estabeleça uma hierarquia entre eles, Landwehr (2001) observa que, dependendo da situação, por exemplo, uma aplicação de *e-commerce*, a disponibilidade e a integridade são mais importantes do que a confidencialidade, que somente assumiria relevância no momento em que se efetivasse o pagamento via cartão de crédito.

A norma ABNT NBR ISO/IEC 17799:2005 (ABNT, 2005) possui 133 controles com 39 objetivos de controle. É composta por 11 seções: Política de segurança da informação; Organizando a segurança da informação; Gestão de ativos; Segurança em recursos humanos; Segurança física e do ambiente; Gerenciamento das operações e comunicações; Controle de acessos; Aquisição, desenvolvimento e manutenção de sistemas de informação; Gestão de incidentes de segurança da informação; Gestão de continuidade do negócio; e Conformidade (com leis, regulamentos e disposições contratuais).

2.3.3 Críticas à Norma ISO/IEC 17799 e às Políticas de Segurança

Apesar da grande aceitação internacional da ISO/IEC 17799, diversos autores tecem críticas a essa norma. Por exemplo, Mikko Siponen (2006), ao criticar a ISO/IEC 17799 e outros padrões relevantes sobre segurança da informação, afirma que essas normas focam

apenas a existência dos processos, não o seu conteúdo, o que não garante que os objetivos dos processos sejam alcançados.

Questionando a eficácia das políticas de segurança em estudo exploratório, Doherty e Fullford (2005b) surpreenderam-se ao concluírem não haver relacionamento estatisticamente significativo entre a adoção de políticas de segurança da informação e a incidência ou severidade de brechas de segurança. A pesquisa foi realizada no Reino Unido; foram obtidas 219 respostas válidas, de 2.838 questionários enviados pelo correio para empresas com mais de 250 pessoas. A taxa de respostas foi baixa, de 7,7%. Surpreendentemente, as 5 hipóteses formuladas foram rejeitadas. As hipóteses eram:

- Existência de uma política de segurança documentada (presumivelmente a existência de uma política de segurança formalizada favorece a diminuição dos incidentes em termos de freqüência e severidade);

- Antigüidade da política de segurança (presumivelmente a antigüidade da política de segurança favorece a diminuição dos incidentes em termos de freqüência e severidade);

- Periodicidade de atualização da política de segurança (presumivelmente a revisão periódica da política de segurança favorece a diminuição dos incidentes em termos de freqüência e severidade);

- Escopo da política de segurança (presumivelmente o escopo mais amplo da política de segurança favorece a diminuição dos incidentes em termos de freqüência e severidade);

- Adoção de boas práticas (presumivelmente a adoção de boas práticas de segurança favorece a diminuição dos incidentes em termos de freqüência e severidade).

Os autores discutem cinco possíveis causas para este resultado:

- Dificuldades com a conscientização; política de segurança não pode ser apenas mais um documento formal, é necessário que haja consciência da segurança entre os funcionários e a administração, o que parece não estar ocorrendo de uma forma geral;

- Dificuldade de imposição; há dificuldade de fazer as pessoas lerem, compreenderem e acatarem as políticas de segurança;

- Padrões muito complexos; o assunto é complexo e multidisciplinar, e os padrões e políticas acabam refletindo esta complexidade;

- Recursos inadequados de monitoramento; em muitos casos, os recursos disponíveis para monitoramento da política de segurança são insuficientes ou inadequados;

- Falha na adaptação à organização; os requisitos de segurança dependem do tipo de informação que a organização processa e da sua cultura organizacional. Em muitas organizações, os padrões (inclusive as políticas de segurança) tendem a ser impostas de maneira homogênea, desrespeitando culturas locais.

Os autores prosseguem sugerindo que não há espaço para complacência na aplicação da política de segurança, que deve permear por toda a organização; as pessoas precisam ser realmente conscientizadas da sua importância. Além disso, as organizações deveriam ser mais

pró-ativas na avaliação da eficácia das suas políticas; quando da ocorrência de falhas, as políticas deveriam ser imediatamente revistas para determinar como estes incidentes poderiam ser evitados no futuro.

A necessidade da implantação de uma "consciência da segurança da informação" é referida por Kruger e Kearney (2006) com base no argumento de que a gestão efetiva da segurança da informação requer uma combinação de controles técnicos e de procedimentos; o valor destes controles usualmente depende de sua implementação e uso corretos, ambos realizados por pessoas. Assim, a implementação de controles de segurança efetivos depende da criação de um ambiente positivo de segurança, onde todas as pessoas realmente compreendam e adotem os comportamentos que delas são esperados.

Apesar destas críticas sobre vários aspectos da norma ISO/IEC 17799, o problema mais sério diz respeito à sua implantação isolada, de forma não articulada com a governança de TI. Balbo (2007) afirma que

> "é muito comum encontrar um cenário onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional e definido pela análise de risco. A responsabilidade pelo nível correto de segurança da informação deve ser uma decisão estratégica de negócios, tendo como base um modelo de Governança da Segurança da Informação que contemple uma análise de risco."

O foco na governança corporativa também passava a exigir conformidade com leis e regulamentos; embora este item seja previsto explicitamente na ISO/IEC 17799, a sua implementação prática é extremamente complexa e tem implicações profundas no desenvolvimento de sistemas (ABNT, 2005).

2.3.4 Segurança e Sistemas de Informação

Existem muitas situações não resolvidas, relacionadas ao desenvolvimento de sistemas, como as apontadas por Landwehr (2001):

- Práticas de programação inseguras (a maior fonte de invasão é relacionada a estouros de *buffer* - programas que escrevem em regiões da memória sem testar o seu tamanho antes);

- Decisões de projeto inseguras, particularmente na camada de aplicação - os sistemas tendem a incorporar módulos bastante poderosos (como, por exemplo, serviço de *e-mail*), capazes de executar outros programas, sem um controle mais rígido; assim, facilmente um usuário pode colocar, indevidamente, à disposição do mundo, de forma inocente ou não, conteúdo estratégico de uma empresa ou mesmo *software* destrutivos;

- Arquiteturas de sistemas complexas e difíceis de gerenciar (os *software* são cada vez mais difíceis de configurar, o que exige trabalho especializado, e acaba servindo como porta de entrada para invasões e uso malicioso).

Os desenvolvedores não foram ainda capazes de gerar sistemas simples de implementar, de baixo custo e de fácil utilização por parte dos usuários. Pelo contrário, os sistemas apresentam tendência de custos, complexidade e dificuldade de uso e de configuração crescentes, e sem um correspondente aumento da segurança. Assim, a tentativa de criar sistemas seguros a partir de módulos inseguros acaba não obtendo sucesso (LANDWEHR, 2001).

Um grande problema parece concentrar-se no desenvolvimento dos sistemas. Mesmo se a infra-estrutura fornece níveis aceitáveis ou eventualmente bons de confidencialidade, integridade e disponibilidade aos dados, a manipulação que os sistemas fazem destes dados parece não corresponder ao que a organização espera da sua informação.

Corroborando esta preocupação com sistemas, Whitman (2004), a partir de pesquisa, cita como as maiores ameaças à segurança da informação, pela ordem: ataques deliberados a *software*; falhas técnicas ou erros de *software*; ato humano de falha ou erro; atos deliberados de espionagem ou transgressão; atos deliberados de sabotagem ou vandalismo; falhas técnicas ou erros de *hardware*; atos deliberados de furto/roubo; forças da natureza; comprometimento de propriedade intelectual; problemas de qualidade em provedores de serviços; obsolescência tecnológica; e atos deliberados de extorsão de informações.

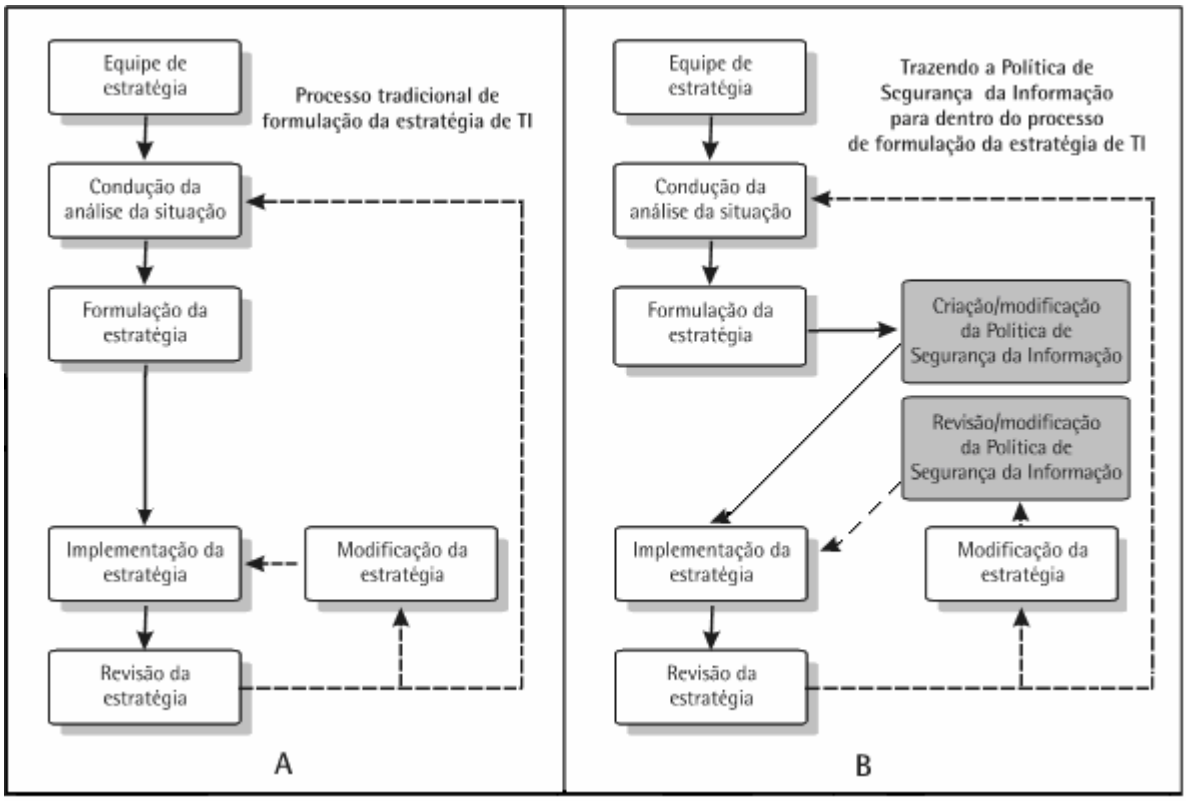

Figura 1 – Do PESI tradicional para o PESI orientado à segurança
(Adaptado de DOHERTY & FULFORD, 2005a)

Visando solucionar os diversos problemas de segurança levantados, Doherty e Fulford (2005a) propõem um modelo de planejamento estratégico de sistemas de informação orientado à segurança (Figura 1).

Segundo os autores, o modelo da Figura 1A representa a maneira tradicional de formulação do PESI: a equipe que formula a estratégia da organização reúne-se, conduz a análise da situação e é formulada e implementada uma estratégia. Tendo sido implementado o novo plano estratégico, ele será periodicamente revisado e modificado para assegurar sua adequação às novas necessidades da organização. No modelo proposto (Figura 1B), este processo tradicional foi modificado para acomodar a política de segurança da informação: após a equipe de estratégia ter conduzido a análise da situação e formulado uma estratégia, seu impacto na política de segurança da informação deverá ser revisto, e a política de segurança modificada, se for o caso, com vistas a adquirir conformidade com a nova estratégia.

De modo análogo, uma vez operacional a nova estratégia, a mesma deverá ser revisada, avaliando seus impactos na política de segurança da informação. A fase de Revisão/modificação da Política de Segurança da Informação (Figura 1B) é considerada pelos autores como a mais relevante no contexto. Esta atividade terá como objetivo avaliar as implicações da segurança na estratégia.

Este grupo avaliará individualmente de que forma cada projeto de TI – documentado no PESI – poderá ser utilizado (e “abusado”, ou seja, ser usado fora das especificações para tentar forçar erros) quando estiver operacional, e de que forma cada um destes projetos poderá constituir uma ameaça à organização.

De posse desta lista de possíveis ameaças, a política de segurança existente deverá ser criticamente avaliada, para verificar como ela trata cada uma destas ameaças, e alterada, se for o caso (DOHERTY E FULFORD, 2005a).

2.3.5 Segurança da Informação e Governança

A Política de Segurança da Informação é um documento (ou coleção de documentos) que formaliza metas, objetivos, ética, direitos e responsabilidades. Possui caráter crítico na prevenção, detecção e resposta a incidentes de segurança. Objetiva *"prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações pertinentes"* (ABNT, 2005).

A estratégia de segurança da informação deve estar alinhada aos objetivos estratégicos definidos pela organização, uma vez que ela dá suporte e sustentação à estratégia competitiva, protegendo os ativos críticos da informação, minimizando riscos operacionais, controlando o ambiente organizacional e dando proteção à vantagem competitiva. A proteção das informações do planejamento estratégico, o suporte à estratégia competitiva e o controle dos ativos e atividades que necessitem de informação são os aspectos organizacionais mais importantes que a política de segurança deve proteger (OLIVA, 2003). Sêmola (2003) afirma que "as ações (relativas à segurança da informação) precisam estar intimamente alinhadas às diretrizes estratégicas da empresa e, para isso, é necessário ter uma visão corporativa, global e ampla".

Von Solms (2006) considera que os aspectos mais importantes, relativos à segurança da informação, são: Sistemas de controle, Conformidade com padrões relevantes, Gestão de riscos, informação precisa, relevante e em tempo hábil, Controles internos, etc.

A governança da segurança da informação é parte integrante da gestão corporativa, e consiste em (VON SOLMS, 2006):

- Gestão e compromisso de liderança do conselho administrativo (se houver) e alta diretoria no sentido de uma boa segurança da informação;

- Presença de estruturas organizacionais que forcem uma boa segurança da informação;

- Uso de conhecimento e comprometimento no sentido de uma boa segurança da informação;

- Todos os esforços necessários, envolvendo políticas, procedimentos, processos, tecnologias e mecanismos de conformidade (*compliance*).

Paralelamente à importância que a segurança da informação vem assumindo nas organizações, diversos autores têm colocado a necessidade de integração de diversos modelos que possuem as “melhores práticas” para a gestão de TI, e a governança de TI passa a englobar esses modelos. Bernardes e Moreira (2005) destacam que, em função da dependência cada vez maior das organizações em relação à TI, estas devem preocupar-se em gerenciar melhor seu ambiente tecnológico, mantendo a infra-estrutura segura e confiável. Os autores citam modelos de “melhores práticas” para a governança da tecnologia da informação,

como COBIT e ITIL e apresentam um modelo cujo objetivo é permitir o alinhamento das questões de Segurança da Informação com o plano estratégico da organização.

No que diz respeito à segurança da informação, o ITIL define alguns documentos (ITIL, 2007):

- Políticas de segurança de informação, que devem partir dos responsáveis da organização, e devem conter:
    - Objetivos e âmbito de segurança de informação para a organização;
    - Metas e princípios de gestão sobre a forma como a segurança de informação deve ser gerida;
    - Definição das funções, e responsabilidades, para a segurança de informação;
- Planos de segurança de informação – descrevem como é que as políticas devem ser implementadas para um determinado sistema de informação e/ou unidade de negócio;
- Manuais de segurança de informação – documentos operacionais para utilização diária com instruções operacionais detalhadas sobre a segurança de informação.

O processo de gestão de segurança ("*Security Management Process*") do ITIL descreve como a segurança da informação se enquadra na gestão da organização.

O COBIT prevê dois objetivos de controle especificamente para a segurança da informação: DS4 - Assegurar a continuidade dos serviços ("*Ensure continuous service*") e DS5 - Assegurar a segurança dos sistemas ("*Ensure systems security*").

A linha de integrar diversos modelos que possuem as "melhores práticas" para a gestão de TI é seguida por documento do "*The IT Governance Institute*" (responsável pelo COBIT) e do "*The Office of Government Commerce*" (responsável pelo ITIL) intitulado "*Aligning COBIT, ITIL and ISO 17799 for Business Benefit*" (ITGI, 2005): "*Como a governança de TI – tanto o conceito quanto a prática efetiva – vem ganhando oportunidade e aceitação, as melhores práticas de TI serão cada vez mais alinhadas ao negócio a aos requisitos da governança, ao invés de se preocuparem apenas com requisitos técnicos. A governança de TI aponta para as seguintes áreas principais:*

- *Alinhamento estratégico, com foco no alinhamento com o negócio e soluções colaborativas;*

- *Entrega de valor, concentrando-se na otimização de custos e comprovando o valor da TI;*

- *Gestão do risco, focando a salvaguarda dos ativos de TI, recuperação de desastres e continuidade de operações;*

- *Gestão de recursos, otimização do conhecimento e da infra-estrutura de TI;*

- *Medição da performance, rastreamento das entregas de projetos e monitoramento dos serviços da TI*".

2.3.6 Fatores Habilitadores e Inibidores do Alinhamento Estratégico da Segurança

Os fatores que determinariam o sucesso da segurança da informação em uma organização, segundo a norma ABNT ISO 17799:2005 (ABNT, 2005), são:

- Política de segurança da informação, objetivos e atividades que reflitam os objetivos do negócio;

- Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

- Comprometimento e apoio visível de todos os níveis gerenciais;

- Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

- Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

- Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

- Provisão de recursos financeiros para as atividades de gestão da segurança da informação;

- Provisão de conscientização, treinamento e educação adequados;

- Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

- Implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

"Conforme Von Solms (2006), fatores habilitadores do enfoque atual da segurança da informação são uma ênfase maior na governança corporativa e na conformidade com leis e regulamentos". Segundo o autor, haveria um comprometimento forte com a precisão e veracidade das informações, por conta de regulamentações cada vez mais exigentes. A prevenção de fraudes pela manipulação de sistemas de informação passa a ser um dos objetivos principais. Grandes riscos são oferecidos pelas pessoas que utilizam os sistemas (diretores, empregados, clientes). A engenharia social (tipo de ataque em que alguém faz uso de persuasão e convencimento, aproveitando-se da ingenuidade ou da confiança do usuário de computador para obter informação indevida) também oferece riscos consideráveis. Atualmente são requeridos mais ferramentas de informação (*report*) formais e mecanismos que permitam à alta administração uma visão precisa e compreensível sobre quais riscos de TI realmente existem e como estes riscos são administrados.

Há diversos fatores relevantes para que a implantação da segurança da informação em uma organização obtenha bons resultados, como os citados por Oliva (2003), obtidos como resultado de sua pesquisa:

- A política de segurança regulamenta os quesitos de segurança na empresa;

- A política de segurança pode ser exigência da Governança Corporativa;

- Na elaboração da Política de Segurança deve estar envolvida a alta administração;

- Devem ser determinados os pontos críticos a serem tratados na Política de Segurança;

- É necessário, antes de elaborar a política de segurança, realizar uma Análise de Risco;

- A Análise de Risco determina os ativos a serem protegidos, determina o impacto financeiro, estima as ameaças e vulnerabilidades e propõe as soluções em ordem de prioridade;

- A Política de Segurança tem a estrutura de pirâmide, tendo no alto as diretrizes, seguidas das políticas específicas e dos procedimentos;

- Para a implantação da Política é necessária a assinatura de termo de responsabilidade, treinamento específico, campanhas de *endomarketing*;

- A conscientização dos colaboradores é primordial para a implantação da Política de Segurança;

- A revisão da política de segurança deve ser realizada anualmente. As empresas que realizam revisões em menos tempo podem ter problemas de definição da Análise de Risco e das políticas específicas. Isso pode ocorrer quando as políticas têm determinações técnicas e não visam ao negócio da empresa.

Por sua vez, Lessa (2006) cita como fatores habilitadores:

- Apoio visível da alta administração;
- Priorização dos aspectos administrativos;
- Política adequada de treinamento;
- Estrutura do projeto organizada através de comitês;
- Iniciativas de mobilização dos funcionários;
- Uso adequado da *intranet* para documentação e restrição de impressões;
- Uso de *e-learning* como ferramenta de treinamento.

Há mais um fator, que é citado apenas por Lessa (2006): a liderança do projeto de implantação da segurança da informação por um executivo que não pertença à área de TI.

Por fim, a Resolução BACEN nº 3.380, de 29/06/2006, que dispõe sobre a implementação de estrutura de Gerenciamento do Risco Operacional, de aplicação específica para as instituições financeiras brasileiras, pode ser considerada fator habilitador, por ser de implementação obrigatória.

Resumidamente, os fatores habilitadores mais citados pelos autores estão listados no Quadro 1 (sem considerar ordem de importância nem a freqüência de citações):

Quadro 1
Fatores habilitadores mais citados

Fator habilitador citado	Autores
Apoio e comprometimento (visíveis) da alta administração	ABNT, 2005; OLIVA, 2003; LESSA, 2006
Ênfase maior na governança corporativa e na conformidade com leis e regulamentos (prevenção de fraudes)	ITGI, 2005; VON SOLMS, 2006; OLIVA, 2003
Estrutura organizacional específica	LESSA, 2006
Conformidade com a cultura organizacional	ABNT, 2005
Provisão dos recursos financeiros adequados	ABNT, 2005
Alinhamento entre política de segurança da informação e estratégia e objetivos do negócio	ITGI, 2005; ABNT, 2005
Gestão de risco (análise/avaliação de riscos e gestão de risco)	ITGI, 2005; ABNT, 2005; OLIVA, 2003
Foco no negócio, não na tecnologia (bom entendimento dos requisitos de segurança da informação, entrega de valor, otimização de custos e comprovação do valor da TI)	ITGI, 2005; ABNT, 2005; OLIVA, 2003; LESSA, 2006
Comprometimento com a precisão e veracidade das informações, por conta de regulamentações cada vez mais exigentes	VON SOLMS, 2006
Conscientização, treinamento, educação e mobilização dos colaboradores de todos os níveis, termo de responsabilidade	ABNT, 2005; OLIVA, 2003; LESSA, 2006
Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação	ABNT, 2005
Medição da performance (implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria)	ITGI, 2005; ABNT, 2005

Os fatores que podem levar ao fracasso da segurança da informação nas organizações tendem a apontar na mesma direção, como citado por Peltier (2002):

- Objetivos da segurança não suportam ou refletem os objetivos ou a missão da empresa;
- A implementação dos controles de segurança contraria a cultura da empresa;
- Falta de apoio visível da diretoria;

- Falta de compreensão do funcionamento dos requisitos de segurança, análise de risco e gestão de risco;

- Divulgação ineficaz da segurança junto aos funcionários;

- Dificuldade dos funcionários em acessar políticas e procedimentos de segurança de forma rápida e eficaz;

- Treinamento inadequado dos funcionários;

- Falta de um programa de medição da eficácia do controle.

2.4 MODELO PRELIMINAR PARA ESTUDO

A literatura sobre alinhamento estratégico, desde o artigo clássico de Henderson e Venkatraman (1993), tem evidenciado a importância de alinhar as estratégias de negócio com as estratégicas de TI. Por outro lado, a literatura e normas reguladoras da segurança da informação, principalmente para determinadas organizações em que a informação faz parte de seus produtos vitais, evidencia a importância de que as políticas de segurança de informação estejam bem suportadas pelas estratégias e práticas de segurança da informação que a TI disponibiliza para a organização (DOHERTY e FULFORD, 2005a). Atualmente, grandes conjuntos de normas e regulamentações encontram-se disponibilizados e estão sendo requeridos obrigatoriamente para as organizações, variando em sua aplicação, níveis e intensidade de promoção conforme o setor e o uso da informação como *core competence* de cada negócio.

O Modelo Preliminar para Estudo apresentado na Figura 2 foi elaborado buscando mostrar as dimensões e elementos conceituais do Alinhamento Estratégico (AE) especificamente na área de Segurança de Informação. Ele contém as dimensões e elementos de AE destacados pela literatura.

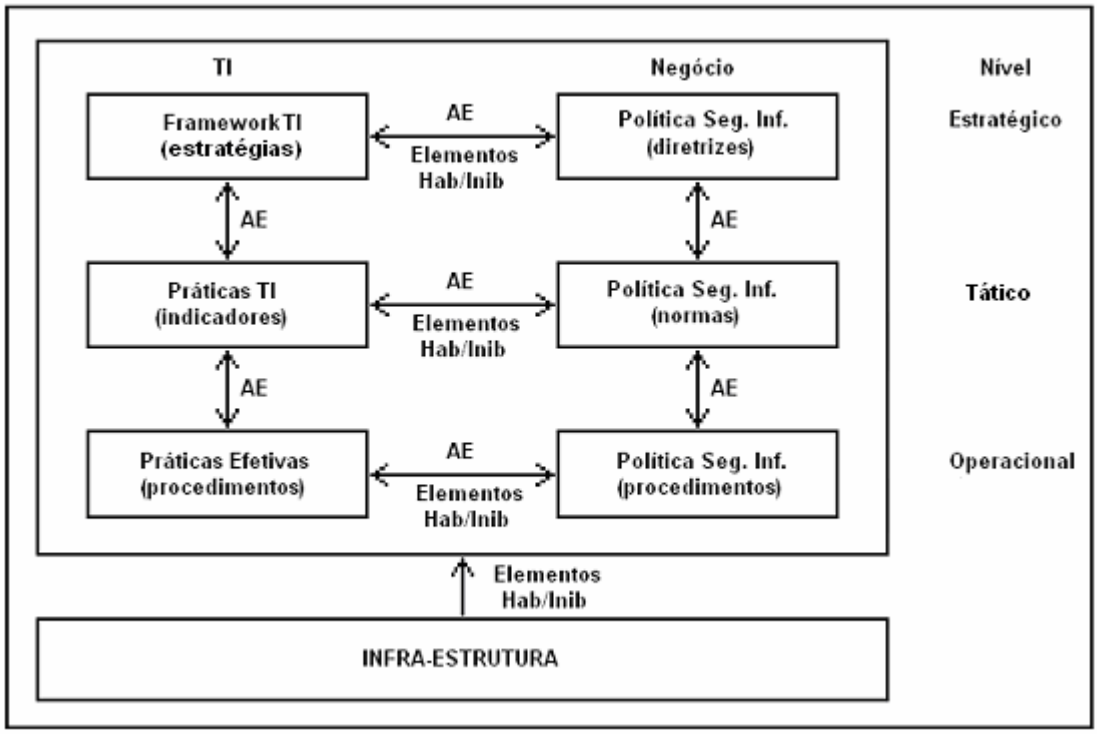

Figura 2 – Modelo Preliminar para Estudo
Fonte: Elaborado pelo Autor

Políticas e estratégias de negócio dependem de decisões em diversos níveis. O´Brien (2001) explica que as decisões em uma empresa normalmente são tomadas com base em três níveis decisórios: (a) **nível de administração estratégica**, composto pelo conselho de diretores, presidente e principais executivos que determinam os objetivos e metas globais, as estratégias a serem seguidas por meio do desenvolvimento de um planejamento estratégico; (b) **nível de administração tática**, composto pelos gerentes de unidades de negócio, que desenvolvem planos de curto e médio prazo, orçamentos, procedimentos e objetivos das

unidades, entre outros aspectos; e, (c) **nível de administração operacional**, composto por gerentes de operações e equipes auto-dirigidas e desenvolve programas de produção, administra recursos e as tarefas de acordo com os procedimentos definidos pela administração tática. Da mesma forma, Henderson e Venkatraman (1993) defendem que o alinhamento estratégico também deve ser promovido em nível estratégico (escopo, competências e governança) e tático/operacional (envolvendo infra-estrutura, processo e habilidades/pessoas).

As **dimensões** consideradas no modelo da Figura 2 são **TI** e **Negócio**, pois a literatura caracteriza o alinhamento estratégico como a adequação estratégica e integração funcional entre as estratégias de negócio e as estratégias de TI (HENDERSON e VENKATRAMAN, 1993). Os **elementos** considerados no modelo da Figura 2 são os níveis **estratégico**, **tático** e **operacional**, conforme amplamente citado na literatura, especificamente por O´Brien (2001).

A Política de Segurança tem a estrutura de pirâmide, tendo no nível estratégico as **diretrizes**, seguidas das políticas específicas (**normas**) no nível tático e dos **procedimentos** no nível operacional (KANAMURA e GEUS, 2002 APUD OLIVA, 2003).

2.4.1 Nível Estratégico

No modelo da Figura 2, o nível **Estratégico** aparece como responsável pela conformidade (*compliance*) com a regulamentação (leis e regulamentos), devendo alinhar-se diretamente com as estratégias do negócio. A política de segurança da informação deve também refletir os objetivos da organização (ABNT, 2005). Conforme Ezingeard et al. (2005), a segurança da informação deve ser gerida de forma a fornecer o máximo benefício para a organização, em alinhamento com os objetivos e a estratégia corporativos.

Neste nível, os elementos habilitadores e/ou inibidores para a dimensão **Negócio**, mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Níveis de segurança da Política de Segurança da Informação (OLIVA, 2003);
- Apoio visível (inclusive financeiro) da alta administração (VON SOLMS, 2006; ABNT, 2005; OLIVA, 2003; LESSA, 2006);
- Impacto no negócio. A norma ABNT ISO 17799:2005 define segurança da informação como "a proteção da informação de vários 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" (ABNT, 2005). A quebra da segurança pode, portanto, ter um grande impacto no negócio, trazer riscos e mesmo inviabilizar o negócio.

Os elementos habilitadores e/ou inibidores para a dimensão **TI**, mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Conformidade com leis, regulamentos e contratos, pois devem ser implementados procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários (ABNT, 2005);
- Efeitos da estratégia corporativa na TI, à medida que a TI é afetada pela formulação de novas estratégias organizacionais (DOHERTY E FULFORD, 2005a);

- TI como ferramenta estratégica, pois as organizações utilizam diversos sistemas informatizados como ferramentas para a implantação da estratégia competitiva (OLIVA, 2003).

2.4.2 Nível Tático

No modelo da Figura 2, o nível Tático ou Gerencial monitora e administra a segurança com base nos indicadores (ABNT, 2006), uma vez que uma gestão efetiva da segurança da informação requer uma combinação de controles técnicos e de procedimentos (KRUGER e KEARNEY, 2006). Na norma ABNT ISO 17799:2005 (ABNT, 2005) encontra-se descrito que um dos fatores habilitadores que contribuem para a implantação da segurança da informação em uma organização é a implementação de um sistema de medição que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

Aqui se enquadra o SGSI (Sistema de Gestão de Segurança da Informação), definido pela Norma ABNT ISO 27001:2006; a qual trata de uma forma de gerenciamento destinada a estabelecer políticas baseadas na análise de risco do negócio, cujo objetivo é definir, implementar, operar, manter e sempre melhorar a segurança da informação (ABNT, 2006). O processo de implantação do Sistema de Gestão da Segurança da Informação resulta na padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas, além da criação de indicadores, registros e da definição de um processo educacional de conscientização da organização e de seus parceiros (MARTINS e SANTOS, 2005).

Neste nível, os elementos habilitadores e/ou inibidores para a dimensão **Negócio**, mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Implementação de um sistema de medição que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria (ABNT, 2005; ABNT, 2006);

- Políticas específicas, como recomendado pela Norma ABNT ISO 17799:2005 (ABNT, 2005), as quais devem abranger política de segurança organizacional, política de classificação e controle de ativos da informação, política de segurança em pessoas, política de segurança física e do ambiente, política de gerenciamento das operações e comunicações, política de controle de acesso, política de desenvolvimento e manutenção de sistemas, política de gestão de continuidade de negócio e política de continuidade.

Os elementos habilitadores e/ou inibidores para a dimensão **TI,** mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Controles de segurança. Devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhoria nos existentes (ABNT, 2005);

- Segurança fazendo parte do ciclo de vida dos sistemas, pois segundo Bernardes e Moreira (2005), as organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas;

- Projetos de TI vistos como ameaças à segurança. Um projeto de TI pode constituir-se numa ameaça à segurança da informação. Landwehr (2001) relaciona diversas situações em que sistemas podem ameaçar a segurança. Para evitar este problema, Doherty e Fulford (2005a) propõem que cada projeto de TI seja avaliado criticamente para identificar as possíveis ameaças que representa.

2.4.3 Nível Operacional

No modelo da Figura 2, o nível **Operacional** é responsável pelos procedimentos. Aqui se torna importante a consciência dos usuários (internos e externos ou clientes) sobre o uso seguro dos recursos de TI postos a sua disposição (ABNT, 2005). A implementação de controles de segurança efetivos depende da criação de um ambiente positivo de segurança, onde todas as pessoas realmente compreendam e adotem os comportamentos que delas são esperados (KRUGER e KEARNEY, 2006).

Neste nível, os elementos habilitadores e/ou inibidores para a dimensão **Negócio**, mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Consciência da segurança da informação (usuários finais dos sistemas), conforme apregoado por ABNT (2005) e Kruger e Kearney (2006);

- Consciência da segurança da informação (clientes), conforme apregoado por ABNT (2005) e Kruger e Kearney (2006);

- Relacionamento com usuários; a norma ABNT ISO 17799:2005 afirma que a política de segurança da informação deve estabelecer direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização; o relacionamento com os usuários precisa ser claro e bem definido (ABNT, 2005).

Os elementos habilitadores e/ou inibidores para a dimensão **TI**, mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo, são:

- Documentação dos sistemas. Normalmente, uma organização desenvolve e adota procedimentos-padrão para a operação dos sistemas de informação. O seu uso promove a qualidade e minimiza as chances de erros e fraude. Isto ajuda tanto os usuários finais como os especialistas de TI a saberem o que é esperado deles em termos de procedimentos operacionais e qualidade dos sistemas. Além disso, as documentações do projeto dos sistemas e *software* e da operação dos mesmos devem ser desenvolvidas e mantidas atualizadas. A documentação é inestimável na manutenção de um sistema à medida que são feitos os melhoramentos necessários (O'BRIEN, 2001). Também a norma ABNT ISO 17799:2005 afirma que os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem (ABNT, 2005).

- Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e devem ser efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação (ABNT, 2005).

- Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários (ABNT, 2005).

2.4.4 Infra-Estrutura

A infra-estrutura engloba todo o *hardware* da organização, os sistemas operacionais, roteadores, redes, serviço de e-mail, bancos de dados, comunicação e assim por diante; em termos de segurança da informação, engloba antivírus, autenticação de usuários na rede e nos demais serviços, detectores de intrusão, *firewall* e outros *software* assemelhados. No caso específico da área bancária, envolve ainda terminais em agências bancárias, *site* na internet, terminais de atendimento automático, etc. (LAUDON e LAUDON, 2004; O'BRIEN, 2001).

Embora o funcionamento correto e adequado desta infra-estrutura seja crítico, Davenport (1998) considera que a avaliação de tecnologias de infra-estrutura é um processo bastante simples, por duas razões:

- Todas as empresas devem proceder a essa avaliação regularmente, e há abundância de material publicado comparando essas tecnologias;

- A aquisição de tecnologias infra-estruturais raramente significa uma vantagem competitiva em si. Telefones e computadores são itens de consumo de massa, e todos têm características similares. Nenhuma empresa será suplantada pela concorrência com uma máquina de fax ligeiramente melhor.

Empresas podem ficar paralisadas em conflitos internos infindáveis sobre a seleção de uma nova plataforma de computador. É improdutivo gastar muito tempo debatendo o mérito de versões essencialmente idênticas de tecnologias. O mais relevante é definir padrões e orientações comuns. É desejável tentar conduzir os executivos para longe desses debates, e possibilitar que todos possam concentrar mais tempo nas questões relacionadas aos procedimentos em uso e nas tecnologias inovadoras (DAVENPORT, 1998).

Os elementos habilitadores e/ou inibidores mais freqüentemente citados na literatura apresentada nos itens anteriores deste capítulo são:

- Diferencial competitivo: Davenport (1998) considera que a aquisição de tecnologias infra-estruturais raramente significa uma vantagem competitiva (embora considere crítico o funcionamento correto e adequado desta infra-estrutura);

- Confiabilidade: segundo Bernardes e Moreira (2005), o crescimento e o sucesso das organizações atualmente estão diretamente relacionados à necessidade de se manter uma infra-estrutura de TI segura e confiável. A norma ABNT ISO 17799:2005 afirma que as redes devem ser adequadamente gerenciadas e controladas, de forma a serem protegidas contra ameaças; deve ser mantida a segurança de sistemas que utilizam estas redes, incluindo a informação em trânsito. (ABNT, 2005)

- Métricas ou indicadores, que são ferramentas projetadas para facilitar a tomada de decisões e melhorar o desempenho e a responsabilidade através da coleta, análise e divulgação de dados relevantes relativos ao desempenho. O objetivo de medir o desempenho é monitorar o status das

> atividades medidas e facilitar a melhoria das mesmas, pela aplicação de ações corretivas, com base nas medidas observadas. As métricas de segurança podem ser obtidas em diferentes níveis numa organização. Métricas detalhadas, coletadas no nível de sistemas, podem ser agregadas e deslocadas para níveis progressivamente mais altos, dependendo do tamanho e complexidade da organização (SWANSON ET AL., 2003).

2.4.5 Dimensões, Elementos e Variáveis de Pesquisa

O Quadro 2, na próxima página, mostra as variáveis preliminares, vinculadas aos elementos (nível **Estratégico**, nível **Tático**, nível **Operacional** e **Infra-Estrutura**) das dimensões (**Negócio** e **TI**), as quais foram utilizadas como base para o levantamento de dados durante a realização dos estudos de caso, nesta pesquisa.

Quadro 2
Dimensões, elementos e variáveis preliminares de pesquisa

Dimensões	Elementos	Variáveis Preliminares	Autores
Negócio	Nível Estratégico	Níveis de segurança	OLIVA, 2003.
		Impacto no negócio	ABNT, 2005; OLIVA, 2003.
		Apoio da diretoria	ABNT, 2005; LESSA, 2006; PELTIER, 2002.
TI	Nível Estratégico	Conformidade	ABNT, 2005; VON SOLMS, 2006.
		Efeitos da estratégia na TI	DOHERTY E FULFORD, 2005a.
		Ferramenta estratégica	OLIVA, 2003.
Negócio	Nível Tático	Sistema de medição	ABNT, 2005; ABNT, 2006.
		Políticas específicas	ABNT, 2005; VON SOLMS, 2006.
TI	Nível Tático	Controles de segurança	ABNT, 2005.
		Ciclo de vida dos sistemas	BERNARDES E MOREIRA, 2005.
		Projetos de TI como ameaça	LANDWEHR, 2001; DOHERTY E FULFORD, 2005a.
Negócio	Nível Operacional	Consciência da segurança da informação (usuário dos sistemas)	ABNT, 2005; KRUGER E KEARNEY, 2006.
		Consciência da segurança da informação (clientes)	ABNT, 2005; KRUGER E KEARNEY, 2006.
		Relacionamento com usuários	ABNT, 2005.
TI	Nível Operacional	Documentação	O'BRIEN, 2001.
		Critérios de aceitação	ABNT, 2005.
		Controles	ABNT, 2005.
Negócio & TI	Infra-Estrutura	Diferencial competitivo	DAVENPORT, 1998.
		Confiabilidade	DAVENPORT, 1998; BERNARDES E MOREIRA, 2005.
		Métricas	SWANSON ET AL., 2003; ABNT, 2005.

3 METODOLOGIA

Neste capítulo são apresentados os procedimentos metodológicos para a realização desta pesquisa, iniciando com a apresentação do tipo de pesquisa, e posteriormente abordando o desenho da pesquisa, as unidades de análise e os procedimentos utilizados para a coleta e análises dos resultados.

3.1 TIPO DE PESQUISA

A presente pesquisa é qualitativa, utilizando estudos de casos múltiplos como ferramenta de investigação. O estudo foi de caráter descritivo e exploratório. A escolha por esta abordagem se deu por esta pesquisa ser uma inquirição empírica que buscou investigar um fenômeno contemporâneo dentro de um contexto da vida real, onde a fronteira entre o fenômeno e o contexto não estava claramente evidente. Por isso foram utilizadas múltiplas fontes de evidência (3 casos, entrevistas), sem o uso de manipulação ou controle (YIN, 2005).

Três tipos de classificação quanto ao objetivo de pesquisa podem ser encontrados na literatura: o **descritivo**, que descreve o fenômeno dentro de seu contexto; o **exploratório**, que trata com problemas pouco conhecidos, objetivando definir hipóteses ou proposições para futuras pesquisas; e, o **explanatório**, que possui o intuito de explicar relações de causa e efeito a partir de uma teoria. Pode existir uma área de sobreposição entre esses tipos (YIN, 2005). Devido ao caráter deste estudo, julgou-se interessante a utilização dos dois primeiros tipos, uma vez que se tratou de descrever o fenômeno pesquisado dentro de seu contexto.

Como não se dispunha de um instrumento de pesquisa consagrado sobre o alinhamento da Política de Segurança da Informação das organizações com as estratégias e práticas de segurança adotadas na TI, mas apenas de um **Modelo Preliminar para Estudo** (Figura 2), foram realizados estudos de caso, pois estes representam a estratégia mais adequada quando são colocadas questões do tipo ‘como’ e ‘por que’, quando o pesquisador tem pouco controle sobre os acontecimentos e quando o foco se encontra em fenômenos contemporâneos, inseridos em algum contexto da vida real. Este método permite o estudo do fenômeno em seu ambiente natural (YIN, 2005; HOPPEN, 1997).

O estudo de casos múltiplos permite confrontar e comparar os casos, bem como produzir resultados mais confiáveis e generalizáveis (BENBASAT, GOLDSTEIN e MEAD, 1987). O presente estudo teve a intenção de levantar aspectos referentes ao alinhamento estratégico da segurança da informação, no ambiente regulamentado das instituições financeiras, buscando aumentar o conhecimento acerca do tema e do contexto, os quais poderão ser abordados em pesquisas futuras. Sendo assim, trata-se de uma pesquisa transversal, onde é levado em conta apenas o momento da pesquisa, sem a preocupação de se traçar a evolução do fenômeno pesquisado.

3.2 DESENHO DE PESQUISA

A pesquisa está dividida em três etapas principais (sendo a primeira conceitual, a segunda aplicada e a terceira, novamente, conceitual), e cada uma destas etapas, subdividida em fases.

A Figura 3 apresenta uma visão geral da pesquisa e representa as suas etapas e fases. Para um melhor entendimento dos procedimentos metodológicos adotados, as etapas e suas fases são descritas nas seções abaixo.

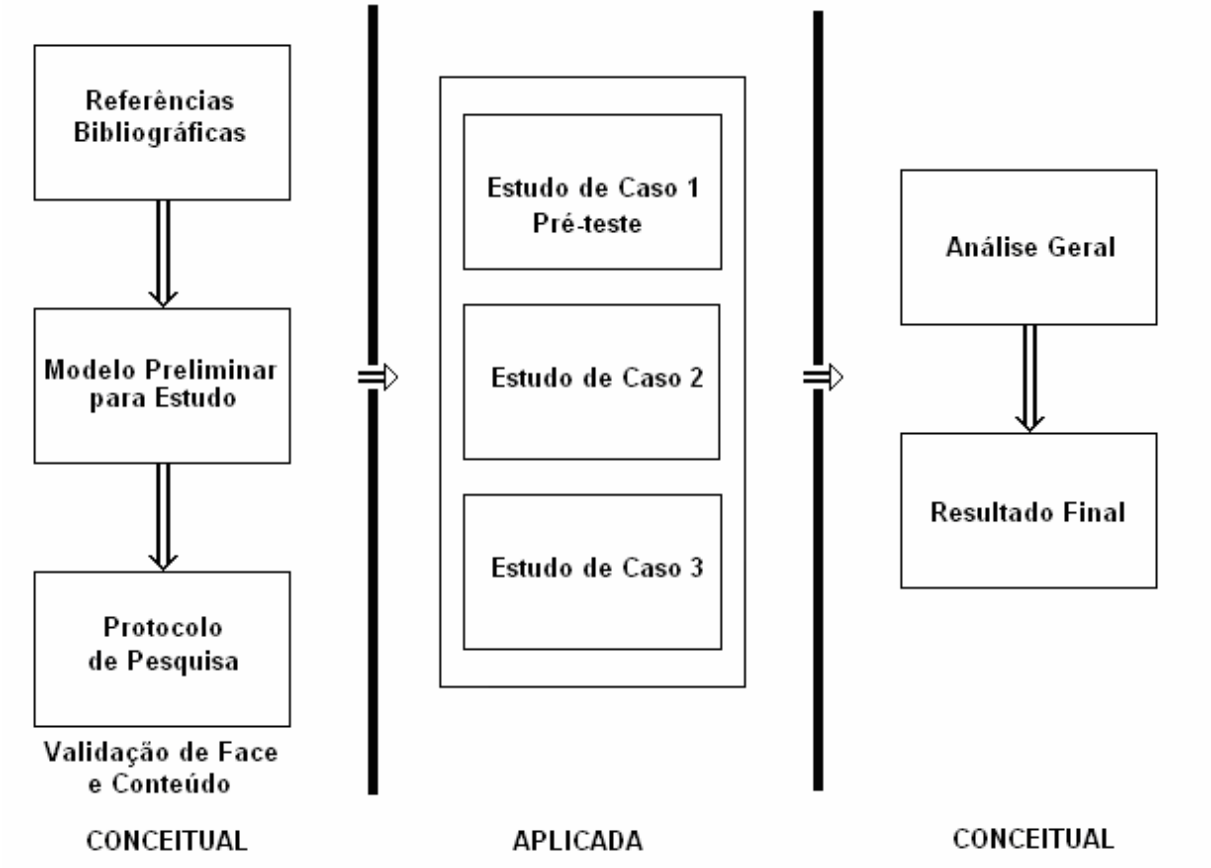

Figura 3 – Desenho de Pesquisa
Fonte: Autor

A primeira etapa, **conceitual**, caracterizou-se por ser de exploração, na qual foram definidos o tema da pesquisa, os objetivos, sua contextualização, a revisão bibliográfica dos principais modelos e conceitos relacionados ao foco da pesquisa, seleção das unidades de análise e elaboração do Modelo Preliminar para Estudo (Figura 2). Em um segundo momento foi validado (face e conteúdo) o roteiro de pesquisa por especialistas (um executivo de TI de um banco regional, um executivo de TI de uma empresa multinacional e um acadêmico).

Na segunda etapa, **aplicada**, ocorreu a coleta de dados nas três organizações selecionadas para estudos de caso – um banco comercial de economia mista, um banco comercial cooperativado e uma instituição financeira pública de fomento, esta última utilizada como caso de contraste.

A terceira etapa, novamente **conceitual**, envolveu a análise geral dos dados coletados pelo pesquisador (qualitativa), a busca pela convergência/divergência dos resultados com o Modelo Preliminar para Estudo e a listagem de fatores habilitadores e inibidores de alinhamento entre a política de segurança da informação e as estratégias e práticas de segurança adotadas pela TI, visando à execução do objetivo principal desta pesquisa.

A seguir, encontram-se descritas em detalhe cada etapa, bem como alguns procedimentos metodológicos como o desenvolvimento e validação do instrumento de pesquisa e a seleção e caracterização das organizações para estudo de caso. A caracterização dos entrevistados encontra-se detalhada na seção de coleta de dados (seção 3.4). Vale destacar que, ao longo dos relatos foram sendo identificados os pontos de validade e confiabilidade que auxiliaram no rigor científico desta pesquisa.

3.2.1 Etapa 1 - Exploração do tema

A primeira preocupação nesta etapa consistiu em definir o tema da pesquisa, no caso o alinhamento estratégico das políticas e estratégias de segurança da informação, bem como seus fatores habilitadores e inibidores. A seguir foram definidos os objetivos da pesquisa e a contextualização do assunto, ou seja, onde seria desenvolvida a pesquisa. Ficou definido que seriam instituições financeiras com atuação no Rio Grande do Sul, de porte médio para

grande, e que tivessem características em comum. Este contexto foi escolhido em função de sua altíssima sensibilidade a problemas de segurança da informação e por ser um setor da economia bastante regulamentado (como, por exemplo, pela Resolução 3.380 do BACEN) e fortemente influenciado pela norma específica de segurança da informação como ABNT ISO 17799:2005. Esta etapa se constituiu de duas fases: revisão da literatura, e desenvolvimento e validade do roteiro de pesquisa.

A revisão de literatura foi ampla e, na realidade, se estendeu ao longo de todo o trabalho, não se imitando a esta primeira fase. Nela foram consultados livros e artigos com as seguintes palavras-chave:

- Alinhamento estratégico;
- Segurança da informação;
- ISO 17799;
- Tecnologia da informação;
- Setor bancário brasileiro;
- Leis que afetam o setor bancário brasileiro;
- Resoluções do BACEN (Banco Central), em especial a 3.380;
- Governança de TI (incluindo ITIL e COBIT);
- Política de segurança da informação.

A partir da revisão bibliográfica foi elaborado o Modelo Preliminar para Estudo (Figura 2), considerando os 3 níveis (estratégico, tático e operacional) e as dimensões “TI” e “Negócio”, observados nos modelos conceituais de O’Brien (2001) e Oliva (2003).

A segunda fase desta etapa, de desenvolvimento e validação do instrumento de pesquisa, iniciou com a concepção de um roteiro preliminar de pesquisa, construído com base na revisão de literatura, cuja versão inicial continha 47 perguntas. Esta primeira versão foi discutida com profissionais das áreas de TI e de Segurança da Informação, professores, mestrandos e doutorandos da área de Sistemas de Informação e de Apoio à Decisão do Programa de Pós-Graduação da Escola de Administração da UFRGS, tendo sido condensada em uma nova versão com 23 questões. Diversas questões foram eliminadas devido a: redundância, falta de clareza, existência de questões marginais e não atendimento direto aos objetivos da pesquisa. Outras questões foram incluídas no instrumento, com base em novas referências bibliográficas relevantes.

Esta versão revisada do roteiro então foi submetida a três especialistas: um especialista em segurança da informação, profissional da área de TI com ampla experiência no tema e em instituições financeiras; uma analista de sistemas com larga experiência e diversas certificações; e, uma professora doutora, com experiência em TI. Estes profissionais avaliaram a compreensão e a relevância das questões, assegurando a validade de seu conteúdo.

A versão final do instrumento de pesquisa ficou apenas com as questões mais relevantes e diretamente ligadas ao Modelo Preliminar para Estudo (Figura 2), relacionadas aos tópicos a serem abordados durante a realização dos estudos de caso (Apêndice C).

3.2.2 Etapa 2 - Execução dos estudos de caso

De posse do instrumento de pesquisa definitivo, teve início o primeiro estudo de caso. Inicialmente, o instrumento foi aplicado em uma instituição financeira comercial de economia mista, visando testar os procedimentos de coleta de dados. Os dados coletados e analisados foram avaliados por um dos entrevistados, alguns resultados reajustados e novamente submetidos. Além deste estudo de caso servir como caso piloto, ficou decidido que ele deveria participar como um dos estudos de casos desta pesquisa.

É importante ressaltar que, em todos os casos estudados, a condição imposta pelas empresas pesquisadas foi o absoluto sigilo quanto à sua identificação. Em nenhuma hipótese, portanto, este pesquisador poderá identificar, nem sequer dar qualquer indicação que permita a identificação das instituições financeiras. A justificativa é totalmente aceitável: a possível divulgação de quaisquer fraquezas ou vulnerabilidades poderia implicar ataques que visassem uma eventual exploração destas instituições, violando as leis e normas de segurança às quais elas estão sujeitas.

Os pré-requisitos da pesquisa eram: a) instituições financeiras consolidadas, estabilizadas, financeiramente sadias e relevantes no contexto nacional; b) sujeitas à mesma regulamentação federal; c) com atuação no Rio Grande do Sul (embora não necessariamente de capital gaúcho); d) tenham implantado, ou estejam implantando, uma Política de Segurança da Informação bem definida, seguindo o padrão ISO/IEC 17799 ou outro; e) duas delas deveriam ser instituições financeiras com contas correntes; f) a outra instituição financeira não poderia ter contas correntes, para funcionar como caso de contraste.

A partir da exigência de sigilo, imediatamente aceita pelo pesquisador, as instituições financeiras pesquisadas passaram a ser identificadas da seguinte maneira:

- Instituição Financeira 1 (**EC1 – Estudo de caso 1**): estudo de caso em instituição financeira de economia mista com contas correntes;

- Instituição Financeira 2 (**EC2 – Estudo de caso 2**): estudo de caso em instituição financeira privada (cooperativa) com contas correntes;

- Instituição Financeira 3 (**EC3 – Estudo de caso 3**): estudo de caso em instituição financeira pública de fomento, sem contas correntes.

Vale destacar que as instituições financeiras que possuem contas correntes (EC1 e EC2) são obrigadas a praticar padrões de segurança muito mais rígidos do que instituições financeiras que não possuam contas correntes (EC3).

3.2.3 Etapa 3 - Análise e conclusões

Na terceira etapa e última etapa desta pesquisa, **conceitual**, foi realizada a transcrição e tabulação dos dados coletados nas entrevistas e pela análise de documentos utilizando o roteiro de pesquisa como padrão de convergência das categorias que levaram aos elementos do modelo e aos fatores inibidores e facilitadores da promoção do alinhamento entre as políticas de segurança da informação e as estratégias e práticas de segurança adotadas pela TI nos níveis operacional, tático e estratégico.

Foi utilizada a técnica de análise de conteúdo das entrevistas e documentos coletados em cada estudo de caso. A Seção 3.5 apresenta os procedimentos utilizados nas análises dos casos.

3.3 UNIDADE DE ANÁLISE

A unidade de análise é representada pelo processo de Alinhamento entre a Política de Segurança da Informação e as Estratégias e Práticas de Segurança Adotadas pela TI nas organizações pesquisadas.

3.4 PROCEDIMENTOS DE COLETA DE DADOS

A pesquisa utilizou como fonte primária de evidências, dados coletados através de entrevistas semi-estruturadas e de observação direta; e, como fonte secundária, a análise de documentos. Os entrevistados foram de três categorias: executivos de negócio e funcionários do banco (normalmente *controllers* e gerentes de agência), executivos de TI de nível estratégico (superintendentes de segurança da informação), tático/operacional (analistas de segurança) e clientes corporativos. Com isto, foram buscadas observações de três pontos de vistas diferentes, permitindo uma melhor triangulação dos dados e confirmação dos fatores habilitadores e inibidores de política de segurança efetivamente ativos.

As entrevistas semi-estruturadas, realizadas com o roteiro de pesquisa como base (Apêndice C), foram a principal fonte de dados; a duração média de cada entrevista foi de cerca de 1 (uma) hora; no caso dos clientes corporativos das instituições financeiras entrevistados, este tempo foi reduzido para cerca de 5 (cinco) minutos, pois havia uma única questão a ser respondida. Vale relembrar que as questões do roteiro tiveram por base variáveis deduzidas da literatura (seção 5.2), vinculadas aos elementos (nível estratégico, nível tático, nível operacional e infra-estrutura) e dimensões (negócio e TI), apresentadas no Modelo Preliminar para Estudo (Figura 2). As informações sobre os entrevistados (experiência, perfil, escolaridade, etc.) encontram-se detalhadas no Capítulo 4.

A análise de documentos (dados secundários) foi utilizada para evidenciar informações que foram obtidas por intermédio de outras fontes (YIN, 2005). No caso dos bancos EC1 e EC2, foi negado o acesso a qualquer documentação interna, sob o argumento de que “é tudo cópia da ABNT ISO 17799:2005”. No entanto, foi fornecido todo o material normalmente colocado à disposição dos clientes dos bancos. Apenas EC3 disponibilizou toda a documentação técnica, a qual ainda está em elaboração, pois a instituição ainda não possui uma Política de Segurança da Informação implantada por completo. Vale lembrar que esta instituição financeira não é comercial, tendo uma política de segurança um pouco diferenciada dos outros casos. Os *websites* das 3 instituições financeiras também foram utilizados como fonte de evidências documentais. A coleta de dados documentais ocorreu concomitantemente com a realização das entrevistas, no período de julho a novembro de 2007.

Uma terceira fonte de dados utilizada foi a observação direta nas empresas, a qual ajuda na complementação das informações coletadas em pesquisas do tipo estudo de caso (YIN, 2005). As observações foram realizadas nas visitas às instalações das instituições. No caso do banco EC1, as 7 entrevistas foram realizadas no ambiente de trabalho, o que permitiu a realização de observações relevantes sobre a organização e dinâmica do setor responsável pela segurança da informação. No caso do banco EC2, as 3 entrevistas foram realizadas em salas de reunião fechadas, dificultando a observação do ambiente, mas permitindo um maior aprofundamento nas questões colocadas aos entrevistados. No caso de EC3 (4 entrevistados), instituição na qual o pesquisador exerce suas atividades profissionais, todos os aspectos puderam ser observados.

Com base nestas três fontes de dados, foi feita a triangulação das informações obtidas, permitindo múltiplas percepções, a partir das várias fontes de evidências utilizadas. Com isto

foi possível tornar as idéias mais claras, tendo em vista a repetição de interpretações e observações dos dados coletados (YIN, 2005).

3.5 PROCEDIMENTOS PARA A ANÁLISE DOS DADOS

A mais importante fonte de dados para a pesquisa foram as entrevistas. Para a análise dos dados coletados foi feita a análise léxica. Segundo Freitas e Janissek (2000), a análise de textos começa pela organização completa do vocabulário utilizado. O léxico é a lista de todas as formas gráficas utilizadas, cada qual estando munida de um número de ordem ou freqüência, ou ainda um conjunto das palavras diferentes utilizadas no texto, com a sua freqüência de aparição. Uma análise léxica inicia pela contagem das palavras, avançando na direção da identificação da dimensão das respostas. No caso de respostas abertas, normalmente são feitas aproximações ou agrupamentos que permitam apresentar critérios mais freqüentemente citados, agrupando palavras afins, excluindo palavras que não interessam, até que se obtenha um conjunto de palavras que represente as principais descrições citadas nos textos. Em resumo, havendo o correto agrupamento das palavras, as freqüências das mesmas possibilitam uma análise de contexto onde as categorias identificadas representem a essência das idéias apresentadas.

A análise léxica pode ser definida como a classificação e contabilização pormenorizada nas freqüências de um vocabulário. As palavras ou expressões podem ser agrupadas de acordo com o seu significado, de modo a subsidiar o pesquisador nesta fase de categorização (BARDIN, 1996 APUD FREITAS E JANISSEK, 2000).

Assim, com o intuito de identificar as palavras ou expressões mais significativas obtidas nas respostas relativas a cada uma das variáveis preliminares (Quadro 2), foi criado

pelo autor um programa de computador, escrito em Visual Basic 6, chamado de “Analisador Léxico” (Figura 4), com as funcionalidades básicas de importar texto, contar palavras, manipular lista de palavras excluídas (tipicamente artigos, pronomes, numerais, preposições e outras) e associar palavras (por exemplo: “alinhamento estratégico”, “segurança da informação”).

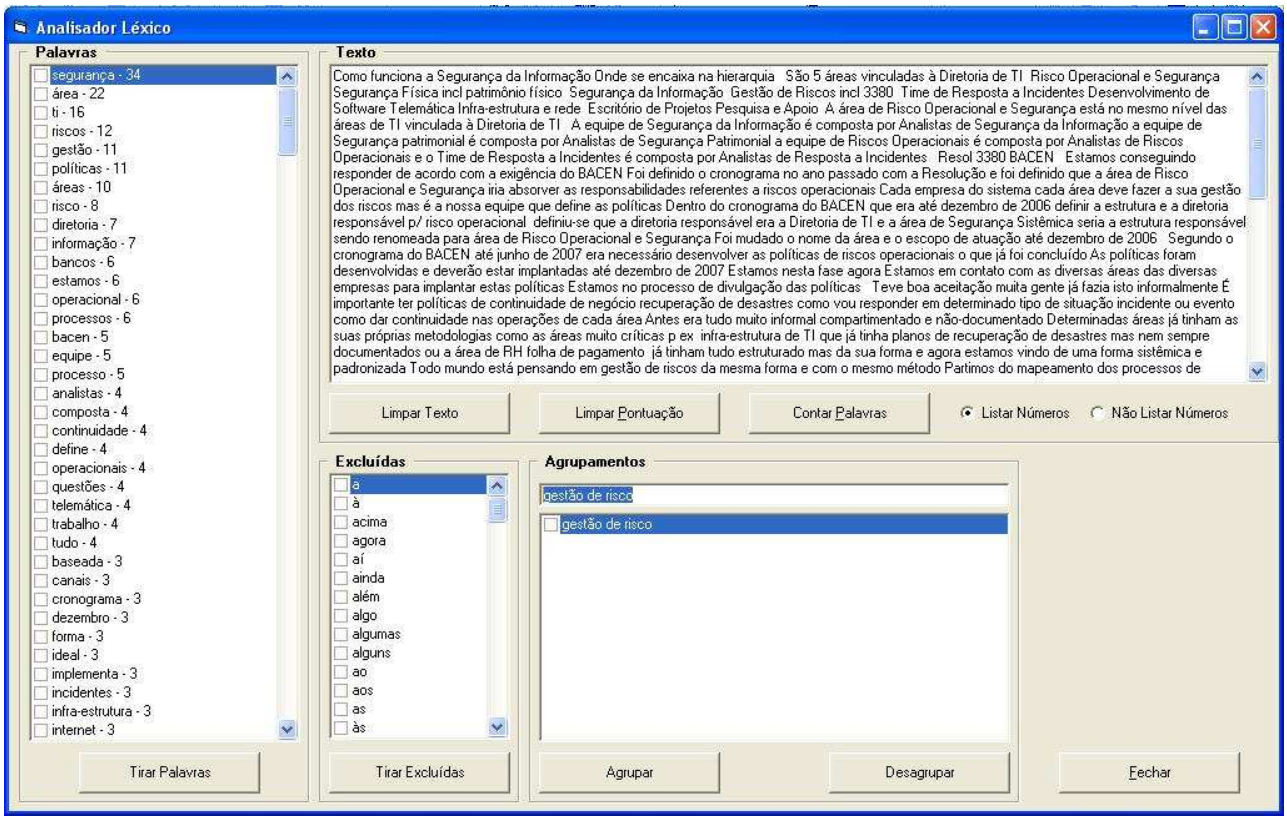

Figura 4 – *Software* “Analisador Léxico”
Fonte: Autor

Numa primeira execução do *software* foram alimentadas todas as respostas obtidas nas entrevistas, incluindo todos os respondentes. O objetivo principal era verificar as respostas obtidas, de forma a gerar a lista de palavras a serem excluídas da análise.

A seguir foram alimentadas no programa todas as respostas relativas a cada uma das variáveis preliminares do instrumento de pesquisa. Em todos os casos, as palavras excluídas foram as mesmas, obtidas na primeira execução do *software*.

As categorias (palavras isoladas ou expressões) encontradas confirmaram, de uma forma geral, as variáveis preliminares, e ainda permitiram que outras variáveis (correspondentes a palavras ou expressões citadas, que se mostraram freqüentes) fossem acrescidas à lista original de variáveis.

3.6 APRESENTAÇÃO DOS RESULTADOS

A análise dos resultados é apresentada no Capítulo 5, da seguinte forma:

a) Convergência dos resultados agrupados entre os Casos 1 e 2, em virtude das grandes semelhanças entre os dois casos. Os resultados foram comparados contra as variáveis do Modelo Preliminar para Estudo (Figura 2);

b) Análise sintética dos principais resultados do caso EC3 (caso contraste), e dos seus resultados comparados contra as variáveis do Modelo Preliminar para Estudo (Figura 2);

d) Apresentação do quadro comparativo dos três estudos de caso realizados;

e) A partir dos dados colhidos nos 3 estudos de caso, foi realizada uma contraposição e uma explicação dos modelos observados com o Modelo Preliminar para Estudo, resultando em um quadro comparativo (Quadro 19) entre as variáveis preliminares

obtidas a partir da literatura e as variáveis confirmadas na prática, a partir da pesquisa.

3.7 CONSIDERAÇÕES SOBRE VALIDADE E CONFIABILIDADE DA PESQUISA

Determinados fatores encontrados em uma pesquisa deste tipo, tais como o contexto qualitativo, a subjetividade dos dados e o uso de múltiplos casos, são tidos como prejudiciais para o rigor cientifico (TRIVIÑOS, 1987). Com a intenção de sanar tais problemas, na realização desta pesquisa foram tomados alguns cuidados e procedimentos que aumentam a validade e a confiabilidade da pesquisa.

3.7.1 Validade

A validade do instrumento de pesquisa utilizado (ver Apêndice C) foi obtida através de seguintes procedimentos:

a) Validade de face, através da revisão feita por profissionais e estudantes de mestrado e doutorado de TI e segurança da informação;

b) Validade de conteúdo, através de revisões feitas por especialistas de TI e segurança da informação.

3.7.2 Validade externa

A validade externa trata do problema de saber se as descobertas de um estudo são generalizáveis, conforme Yin (2005). Os seguintes aspectos da pesquisa contribuíram para a sua validade externa:

a) Escolha de um setor da economia sujeito a forte regulamentação governamental, o que causa uma grande padronização e possibilita a generalização das conclusões para este setor específico (não se tem a pretensão de generalizar as conclusões para outros setores da economia);

b) Escolha de instituições financeiras consolidadas e representativas no cenário nacional;

c) Escolha de instituições financeiras que possuam uma Política de Segurança da Informação institucionalizada, ou estejam em fase de implantação da mesma;

d) Os entrevistados possuem experiência nas empresas, e em cada instituição financeira pesquisada pelo menos um deles esteve diretamente envolvido na definição e implantação da Política de Segurança da Informação.

Além disto, buscou-se reforçar a validade externa desta pesquisa a partir da realização estudos de casos múltiplos e, apesar das particularidades de cada instituição financeira, do estudo ter se mostrado replicável (principalmente nos casos EC1 e EC2).

3.7.3 Confiabilidade

A validade de construto e a confiabilidade podem ser reforçadas se forem atendidos três princípios (YIN, 2005):

a) A utilização de várias fontes de evidências: nesta pesquisa foram utilizadas três fontes de evidências; entrevistas, análise de documentos (quando possível) e observação direta durante as visitas às instituições financeiras;

b) A criação de um banco de dados para os estudos de caso: todos os arquivos de áudio obtidos através de gravação das entrevistas com gravador digital estão arquivadas, assim como os documentos, materiais de esclarecimento ao cliente, anotações diversas e rascunhos; todo o material coletado na pesquisa poderá ser novamente analisado no futuro;

c) O encadeamento das evidências: a descrição dos casos seguiu a seqüência definida pela teoria; ao longo do texto foram apresentadas evidências de cada aspecto, através de trechos de entrevistas, observações realizadas e documentos fornecidos.

4 ESTUDOS DE CASO

Cada um dos 3 (três) estudos de caso está estruturado da seguinte maneira: são apresentadas as empresas e caracterizados os entrevistados; posteriormente é apresentado o contexto organizacional; são apresentadas as observações realizadas, a partir das visitas, da análise da documentação e das entrevistas realizadas, abordando a segurança da informação nos níveis estratégico, tático e operacional, bem como a infra-estrutura.

4.1 ESTUDO DE CASO 1

O Estudo de Caso 1 refere-se a um banco de economia mista, com contas correntes com acesso via *internet banking* e ampla rede de ATMs (*Automated Teller Machine*), conhecidos como terminais de auto-atendimento. Nesta empresa, os entrevistados encontram-se representados por (Quadro 3):

Quadro 3
Entrevistados de EC1

Pessoa	Setor	Cargo/Função
SSI	Superintendência de Segurança da Informação	Superintendente de Segurança da Informação
GSI	Superintendência de Segurança da Informação	Gerente de Segurança da Informação
ASI	Superintendência de Segurança da Informação	Analista de Segurança da Informação
NA	Controladoria – Gestão da Informação	Analista de negócios
GP	Gerência de Posto Bancário	Gerente de Posto Bancário
CL1		Cliente 1 (pessoa física)
CL2		Cliente 2 (pessoa física)

4.1.1 Contexto Organizacional

EC1 é uma instituição financeira que atua como banco múltiplo nas carteiras: comercial, crédito de financiamento e investimento, crédito imobiliário, desenvolvimento, arrendamento mercantil e investimentos. A diretoria é escolhida de acordo com critérios políticos.

Existe um Comitê de Gestão de TI, composto por representantes das unidades de Segurança da Informação, Infra-estrutura de TI e Sistemas, que discute os assuntos relativos à TI e assessora a Vice-Presidência, à qual as três unidades estão subordinadas.

A área de Segurança não define tecnologia, só estabelece princípios e define requisitos de segurança; a metodologia de desenvolvimento da área de Sistemas inclui normas de segurança. A área de Segurança não audita sistemas, apenas realiza visitas técnicas e diligências técnicas; existe uma parceria forte com uma consultoria no que diz respeito à segurança da informação e continuidade.

O caráter estratégico da Segurança da Informação é claro e explícito para esta empresa, conforme expressa o entrevistado GSI em seu depoimento: “É um jogo pesado. É uma área de segurança estratégica”.

4.1.2 Segurança da Informação – Nível Estratégico

A Política de Segurança da Informação para esta empresa encontra-se constituída em 3 níveis (estratégico, tático e operacional), conforme explica o entrevistado SSI,

> O Nível Estratégico onde tem a resolução da diretoria com os princípios ou diretrizes; o Nível Tático onde temos as normas gerais para administradores técnicos e usuários; e o Nível Operacional com as normas específicas.

O entrevistado prossegue dizendo que,

> nós desenvolvemos todos os níveis. Nós publicamos todos os níveis da política. Primeiro publicamos as diretrizes em nível estratégico; são 10 diretrizes, e depois abrimos todos os outros níveis. A política está em consolidação; ela foi construída como um Lego, onde as partes são encaixadas enquanto vamos correndo as questões dentro das unidades do banco. O banco é muito grande, vamos melhorando a política, e ela consolida neste sentido. Ela atende todos os níveis: estratégico, tático, e agora estamos passando para o nível operacional, com o braço em cima do plano de contingência de negócio.

A partir da análise de documentos e dos relatos dos entrevistados constata-se que a Política de Segurança de Informação é baseada na ABNT ISO 17799:2005; existe uma resolução da diretoria com os princípios, e diversas instruções normativas que implementam a resolução, porém ainda incompleta, conforme depoimento do entrevistado GSI, "a aderência à ISO 17799: 60% total, 31% parcial". A informação é classificada em: confidencial, restrita, interna e pública.

Qualquer impacto relativo à quebra de segurança é crítico no negócio, afirma o entrevistado SSI. O entrevistado ASI complementa:

> A quebra de confidencialidade das informações pode resultar num grande impacto para a imagem pública da empresa; a alteração indevida de informações pode implicar a perda de credibilidade da instituição diante de seus clientes; a indisponibilidade das informações certamente resultará na perda de negócios, em especial, o *homebanking-officebanking* e o comércio eletrônico,

O apoio da Diretoria à Segurança da Informação é claro e explícito, conforme expressa o entrevistado SSI: "A diretoria apóia ativamente [a Segurança da Informação], com claro direcionamento e demonstrando comprometimento. A primeira atitude foi a criação da unidade de Segurança de TI". Vale destacar que esta unidade encontra-se vinculada à Vice-Presidência, evidenciando o caráter e importância estratégica ao tema. "A Diretoria tem dado a prioridade para os projetos que envolvem segurança.", complementa o entrevistado ASI.

Assim como estas, outras ações para segurança da informação citadas e observadas através da análise de documentos são: a participação na autoridade certificadora e o alinhamento com a Resolução 3380 do BACEN.

Este caráter crítico atribuído à conformidade da segurança da informação com leis, regulamentos e contratos é confirmado pelo entrevistado SSI, ao citar que o "alinhamento da Resolução 3380 do BACEN (Basiléia II) como prioridade das ações da estratégia do Banco." Em outro momento da entrevista, o entrevistado ressalta que,

> o banco está muito orientado às questões da Segurança. A Resolução 3380 está dentro da Controladoria, mas a parte relativa à Segurança está com a Segurança de TI. A Resolução 3380 possui várias frentes; a frente de Segurança, que atinge toda a parte de informática, está dentro da Segurança de TI.

Sempre há um risco de que a formulação de uma nova estratégia organizacional afete a TI e a segurança da informação, conforme expressa o entrevistado SSI: "Sempre as estratégias organizacionais de nosso banco levam em conta o alinhamento com a TI e segurança da Informação. Isso é feito através da gestão dos diversos comitês e pelo comitê estratégico". Segundo o entrevistado este é um ponto forte das políticas do banco. Porém, outro entrevistado, o ASI, alerta que se deve cuidar com mudanças rápidas porque "Certamente a dependência de uma adequação muito rápida será necessária para assimilar a nova estratégia". Existem, obviamente, situações que exigem alterações estratégicas muito rápidas, o que pode sem dúvida comprometer a segurança. Mas a situação, pelo que se deduz das entrevistas, parece estar sob controle.

Os principais Sistemas de Informação utilizados por este banco são: Sistema de Gestão (ERP), Sistema de Informação Executiva (EIS) e Site institucional/*Internet Banking*. Nenhum dos entrevistados, quando questionado, conseguiu relatar como cada um deles dá suporte à

estratégia competitiva da empresa nem como cada um deles suporta a segurança da informação.

4.1.3 Segurança da Informação – Nível Tático

A avaliação que a empresa faz da segurança da informação neste nível, ou seja, das métricas utilizadas, não diz respeito a avaliações sobre desempenho, disponibilidade e confiabilidade da infra-estrutura; mas diz respeito a como a empresa avalia a adequação das normas de segurança da informação às estratégias empresariais e regulamentações pertinentes. Quando entrevistado, ASI explica que “Existe uma Auditoria Externa contratada que faz a verificação do desempenho e da adequação às conformidades estabelecidas”, procedimento este que ele considera como sendo um ponto forte. A área de Segurança da Informação avalia perdas financeiras evitadas, confrontando com situações anteriores; medida esta que traz prestígio junto à diretoria e aos colegas, segundo o entrevistado GSI. Apesar disto, a aderência à ABNT ISO 17799:2005 é 60% total, 31% parcial, complementa o entrevistado.

A área GSI diz que a área (de Segurança da Informação) avalia perdas financeiras evitadas, confrontando com situações anteriores; ainda, segundo GSI, uma medida é o prestígio junto à diretoria e aos colegas.

As principais políticas de segurança de informação em nível tático específicas para esta empresa em ordem de prioridade nas citações das entrevistas, são:

Quadro 4
Principais Políticas de Segurança de Informação de EC1

Ordem	**Política de Segurança da Informação**	**Citação**
1	Conformidade com a legislação e cláusulas contratuais	SSI; ASI
2	Gestão da continuidade do negócio	SSI; ASI
3	Conseqüências da violação da política de segurança	ASI
4	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa	SSI; ASI
5	Detecção e prevenção de vírus e *software* malicioso	ASI

Segundo o entrevistado ASI, a política de segurança da informação explicita quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas "de forma genérica; pois os controles e procedimentos são estabelecidos nas normativas específicas ou nos manuais dos respectivos sistemas". De qualquer forma, todos os entrevistados consideram tal incorporação como sendo um ponto forte.

A segurança da informação faz parte do ciclo de vida dos sistemas na visão do entrevistado SSI quando cita que ela deve fazer parte "em todo o ciclo, desde a fase de planejamento até operação, visando minimizar riscos de falhas". "Os sistemas seguem as normas estabelecidas, ou seja, a referência de segurança está nas normativas", afirma o entrevistado ASI. Porém, do ponto de vista do entrevistado GSI as considerações sobre o assunto são: "a Área de Segurança não define tecnologia, ela só estabelece princípios, ela define requisitos de segurança. A metodologia de desenvolvimento da área de Sistemas inclui normas de segurança". Ele continua dizendo que "há um bom relacionamento entre TI/Segurança". E exemplificando a forma utilizada para a segurança da informação dos sistemas, ele complementa que "existe um módulo único de controle de acesso, que controla

as requisições de cada sistema às rotinas dos outros sistemas". Vale destacar que, durante o período das entrevistas, a área de Sistemas desta empresa estava implantando o padrão de Governança de TI, chamado ITIL.

Quando os entrevistados deste nível de segurança de informação foram questionados sobre avaliação dos projetos de TI, as respostas foram: "Cada projeto de TI é avaliado para saber de que forma pode se constituir numa ameaça à segurança da informação" (SSI), afirmando ser este um ponto forte; "Esta avaliação ainda não está sendo feita de forma conjunta entre área gestora do sistema, auditoria e segurança. A princípio, somente a área gestora do sistema faz uma avaliação individualizada" (ASI), afirmando não considerar um ponto forte, expressando uma opinião contrária ao anterior.

4.1.4 Segurança da Informação – Nível Operacional

O banco investe muito esforço e recursos financeiros na conscientização dos seus colaboradores (usuários finais dos sistemas) sobre segurança da informação e no uso seguro dos sistemas. Os treinamentos visam a "divulgação da Política de Segurança, treinamentos específicos, palestras internas e externas e campanhas mercadológicas de segurança" expressa SSI, sendo que "estão sendo efetuados treinamentos tanto a nível gerencial quanto a usuários estagiários" (ASI). Somente "em 2006 foram realizadas mais de 3.000 horas de treinamento em segurança da informação, página na *Intranet*, evento sobre direito eletrônico" (GSI).

> Existe treinamento diferenciado p/ gerentes, funcionários, caixas e estagiários. Atualmente está havendo um pouco mais de investimento em treinamento. Estagiários e funcionários novos recebem treinamento. Gerentes recebem treinamento/seleção/provas (GP).

No entanto, existe um menor grau de investimento nas pessoas que trabalham como caixas: “Existem cursos periódicos p/ todos (exceto p/ caixas); os caixas recebem pouco treinamento e não têm nenhuma visão do Banco” (GP). Os usuários

> são instruídos a ler toda a norma da instituição referente ao assunto, conforme termo assinado, comprometendo-se a tomar conhecimento e cumprir as mesmas. Também são constantemente enviadas dicas e lembretes através da *intranet* para que os usuários não esqueçam das normas de segurança, e também possam se atualizar quanto ao surgimento de novas ameaças (NA).

Porém, todos os entrevistados são unânimes em considerar como ponto forte.

Os clientes do banco são esclarecidos sobre o uso seguro dos recursos de TI colocados à sua disposição, principalmente, através da *Web* (site corporativo com *Internet Banking*), o que é uma prática da maioria dos bancos atuantes do mercado. As formas utilizadas são informações na *Web* e campanhas de marketing, *folders* e cartazes, palestras externas, cita o entrevistado SSI. No entanto, “Quando existe algum incidente, ocorre uma breve explanação [com o cliente]. Existe uma pretensão de criar um projeto de aculturamento de clientes, sobre os aspectos e recursos de segurança no uso de TI”, explica o entrevistado ASI sobre como são tratados os incidentes. Além de o entrevistado GP concordar com as informações dos colegas (informações no site e panfletos nas agências), ele ainda explicita que, em caso de problemas, os clientes têm suporte rápido, na pessoa do seu Gerente de Contas. Todos os entrevistados consideram tal prática como sendo um ponto forte.

No entanto, a visão dos usuários, embora não seja unânime, conflita um pouco com esta visão otimista dos integrantes da empresa. Quando entrevistado, CL1 diz que,

> não tenho conhecimento de como outros clientes estão informados sobre o assunto, mas pelas informações que aparecem na página do banco, parece existir uma política razoável de esclarecimento e orientação neste assunto. Seguindo as orientações do banco, me parece, no mínimo, razoável.

Já o entrevistado CL2 tem uma postura mais crítica ao afirmar que “Não há esclarecimento algum, além de algumas poucas informações no site do banco na Internet. É um ponto fraco”.

Para o entrevistado AN, “A política [de segurança da informação] estabelece direitos e responsabilidades, inclusive limites a terceirizados e estagiários”. Quando analisada a documentação e o site, constatou-se a existência de um termo de compromisso para o uso de sistemas, informações e recursos de TI da empresa. Este também foi considerado ponto forte pelos entrevistados internos.

A documentação dos sistemas é responsabilidade da Área de Desenvolvimento. Existe controvérsia entre os respondentes quanto a isto, pois o entrevistado SSI considera como sendo ponto forte, enquanto que o entrevistado ASI considera ponto fraco.

Existe um ambiente específico de desenvolvimento de sistemas, o que é uma das boas práticas apontadas pela ABNT ISO 17799:2005, e uma prática de mercado há muitos anos. Para a aceitação de novos sistemas, atualizações e novas versões, existe uma comissão que avalia o desenvolvimento ou as mudanças dos mesmos. Além disto, é feito um acompanhamento de todos os estágios. Também considerado um ponto forte pelos entrevistados internos.

Existem controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança, conforme explica o entrevistado ASI quando diz que,

> existem sistemas específicos para estes tipos de controles. Por exemplo, o sistema de IPS-IDS faz a detecção e prevenção contra tentativas de invasão e outros tipos de ataques. O sistema de antivírus também trabalha de forma preventiva. Existe um sistema de gerenciamento.

Considerando o controle de detecção um ponto forte, a importância da prevenção e detecção de invasões para o negócio é ressaltada pelo entrevistado ASI: “Prevenir e detectar invasões são ações que remetem diretamente à garantia dos negócios”.

Parece não haver, no entanto, procedimentos adequados para a devida conscientização dos usuários. Embora o entrevistado SSI diga que eles existam e considera este um ponto forte, mesmo sem citar nenhum caso, o entrevistado ASI cita que “Infelizmente não temos uma estrutura com recursos de pessoal, suficiente para fazer este trabalho de conscientização. Um trabalho mais dedicado é feito em momentos de ocorrência de um incidente”, considerando este um ponto fraco.

4.1.5 Segurança da Informação – Infra-estrutura

A avaliação de novas tecnologias de infra-estrutura, no que diz respeito à segurança da informação, “é feita em laboratório ou ambiente de homologação. As pesquisas procuram validar o uso das novas tecnologias acopladas aos sistemas existentes. Certamente as novas tecnologias demandarão em manutenções específicas para cada sistema”, segundo o entrevistado ASI. Ele ressalta a importância da infra-estrutura quando cita que “A análise minuciosa do esquema de rede é fundamental na implementação de qualquer projeto de segurança”. Complementando, o entrevistado GSI esclarece que “A área de Segurança não define tecnologia, só estabelece princípios”. Não há referências a ser um diferencial competitivo.

O entrevistado SSI considera a confiabilidade, segurança e estabilidade da infra-estrutura do banco como um ponto forte, o que “garante a continuidade do negócio”, da

mesma forma que o entrevistado ASI quando explica que “qualquer tipo de instabilidade, falta de segurança ou perda da confiabilidade afetará toda a empresa e conseqüentemente a imagem pública. Além do prejuízo em relação à imagem, também gerará um prejuízo financeiro”.

As avaliações operacionais da infra-estrutura (disponibilidade, etc.) são realizadas pela área de Infra-estrutura, não de Segurança da Informação. Segundo o entrevistado ASI, “As métricas são os melhores indicativos para termos uma referência do que está mais crítico e deve ser prioritariamente analisado, e seguir, definida uma estratégia de segurança”.

4.2 ESTUDO DE CASO 2

O Caso de Estudo 2 se refere ao banco de uma das cooperativas de crédito brasileiras, com atuação no Rio Grande do Sul. O banco possui contas correntes. Os entrevistados encontram-se relacionados no Quadro 5.

Quadro 5
Entrevistados de EC2

Pessoa	Setor	Cargo/Função
CSI	Segurança da Informação	Coordenador de Segurança da Informação
AS	Desenvolvimento de *Software*	Analista de Sistemas
CL1		Cliente 1 (pessoa física)

4.2.1 Contexto Organizacional

Este é um banco cooperativo privado, que atua como instrumento das cooperativas de crédito para acessar o mercado financeiro e programas especiais de financiamento,

administrar em escala os recursos do sistema cooperativo, desenvolver produtos corporativos e políticas de comunicação e *marketing*.

O órgão mais alto do sistema é o Conselho Deliberativo, composto por alguns dirigentes de todo o país; deste Conselho Deliberativo emanam políticas para todo o sistema cooperativo, não apenas o banco. A área de Segurança do banco tem cerca de 3 anos. Nasceu na TI (como é comum nos bancos), quando se tornou necessária uma estrutura de segurança para tratar de todos os assuntos relacionados. As áreas vinculadas à Diretoria de TI são:

- Risco Operacional e Segurança (Segurança Física, que inclui patrimônio físico; Segurança da Informação; Gestão de Riscos, que inclui a Resolução BACEN 3380; e Time de Resposta a Incidentes);
- Desenvolvimento de *Software*;
- Telemática (Infra-estrutura e rede);
- Escritório de Projetos;
- Pesquisa e Apoio.

A área de Segurança da Informação desta instituição financeira trabalha no formato de consultoria, envolvendo-se em cada novo projeto de TI, fazendo a avaliação de processos, recomendando as melhores práticas. Há uma interação constante da Segurança da Informação com cada novo tipo de produto, sistema, projeto que é lançado.

4.2.2 Segurança da Informação – Nível Estratégico

A empresa não usa o nome "Política", usa "Regulamento de Segurança da Informação", que é baseado na ABNT ISO 17799:2005 e constituído em 3 níveis (estratégico, tático e operacional). No nível estratégico, existem as diretrizes de segurança da informação (as linhas mestras); no nível tático, existem as normas (uso de e-mail, uso de internet, controle de acesso, classificação da informação); no nível operacional existem procedimentos, chamados de instruções de segurança. É uma política corporativa, válida p/ todo o sistema, ditada pelo Conselho Deliberativo. Conforme explica CSI, "As políticas essenciais, de acordo com as diretrizes das normas ABNT ISO 17799:2005 e ABNT ISO 27001 adaptadas a estrutura de organizacional e de segurança, já foram implantadas". A informação é classificada em: confidencial, uso interno (privada e geral) e irrestrita.

Qualquer impacto relativo à quebra de segurança é crítico, segundo CSI, para quem o mesmo ocorre em qualquer instituição financeira. Na opinião do entrevistado, o pior impacto seria um comprometimento da "disponibilidade", que afetaria a imagem da empresa. Ele prossegue, afirmando que,

> são definidos processos e procedimentos para continuidade: replicação da estrutura de *datacenter*, equipe de recuperação de desastres, planos de ação no caso de indisponibilidade de serviços. Para os serviços críticos, principalmente canais de atendimento, tem infra-estrutura de TI como contingência, que está documentada de acordo com as políticas, tem procedimentos de continuidade operacional (instruções para as pessoas), procedimentos de recuperação de desastres.

Ainda no que diz respeito ao impacto relativo à quebra de segurança, no que diz respeito à confidencialidade e integridade, a situação é similar à dos outros bancos: impera a Lei do Sigilo Bancário, o que requer um tratamento adequado do cadastro de clientes e dos seus dados financeiros. O mesmo entrevistado prossegue afirmando que "temos uma norma de privacidade; outros componentes ajudam a resguardar, como a classificação da informação

(o cadastro de clientes é classificado como confidencial)". O entrevistado SI complementa: "utilizamos a implementação de códigos-fonte com armadilhas para desvios financeiros. Em qualquer um dos casos, o impacto de um problema de segurança da informação é crítico".

A unidade de Segurança da Informação encontra-se subordinada diretamente à Diretoria de TI. A diretoria é a patrocinadora de todas as ações de segurança. O entrevistado CSI afirma que, "[A diretoria] participa de todas as ações relacionadas à *delivery* de novas políticas, aprovação de novos controles, estratégias de gestão e de divulgação em segurança da informação. As principais ações são apoio e gestão da área de segurança".

A contribuição da segurança da informação com vistas a garantir conformidade com padrões relevantes, regulamentações governamentais (BACEN, p.ex.) e contratos, é feita pela utilização de boas práticas de segurança da informação, as quais, segundo SI, garantem,

> um nível de segurança suficiente para a instituição, podendo-se considerar tais atitudes como um ponto forte. Diversos dos itens de conformidade exigidos por órgãos reguladores do sistema financeiro nacional são assegurados através de controles existentes nas políticas de segurança da empresa, que são baseadas nestas normas e outros *frameworks* mundialmente utilizados. Podemos considerar este aspecto como um ponto forte.

O risco de a formulação de uma nova estratégia organizacional afetar a TI e a segurança da informação sempre está presente. O entrevistado prossegue, explicando que,

> se a estratégia tiver alinhamento com a segurança da informação desde o seu início não surgem maiores problemas; neste caso podemos considerar um ponto forte. Do contrário, fatores de segurança não observados no princípio podem impactar na estratégia organizacional. Se a estratégia desenvolvida não estiver alinhada com as normas e boas práticas, automaticamente atingirá a TI e a segurança da informação envolvida – de forma a tornar vulneráveis essas estruturas (SI).

É interessante ressaltar que ambos os entrevistados expressam a opinião de que a estratégia é que tem de estar alinhada com a segurança, e não o contrário.

Os sistemas principais em uso na instituição financeira são: o Sistema de Gestão desenvolvido localmente (ERP – plataforma considerada um ponto forte nas suas aplicações, mas enfraquecida pela limitação tecnológica oferecida pelas linguagens utilizadas); o Sistema de Relacionamento (CRM); e, o Site institucional/*Internet Banking*. Estes dois últimos sistemas podem ser considerados pontos fortes, na opinião dos entrevistados CSI e SI.

4.2.3 Segurança da Informação – Nível Tático

O banco avalia o desempenho da gestão da segurança da informação a partir do resultado de auditorias e histórico de incidentes. Embora não existindo um sistema de medição formal para a avaliação da segurança da informação, o entrevistado CSI considera que "este é um ponto forte e essencial para a melhoria contínua do sistema de gestão de segurança da informação". Por outro lado, o entrevistado SI possui um ponto de vista discordante, quando explica que,

> muitas vezes, se considera [a segurança da informação] como um fator atrapalhador no desenvolvimento do negócio. No entanto, com a conscientização constante, essa visão tende a se modificar com o tempo. Esse ponto pode ser considerado fraco em relação à segurança da informação.

Há uma discordância entre os entrevistados na ordenação das principais políticas de segurança de informação em nível tático, conforme apresentado no Quadro 6.

Quadro 6
Principais Políticas de Segurança de Informação de EC2

Ordem	Política de Segurança da Informação	Citação
1	Conformidade com a legislação e cláusulas contratuais	CSI
2	Gestão da continuidade do negócio	CSI
3	Detecção e prevenção de vírus e *software* malicioso	CSI
1	Detecção e prevenção de vírus e *software* malicioso	SI
2	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa	SI
3	Conformidade com a legislação e cláusulas contratuais	SI

Conforme evidenciado pelo entrevistado CSI, a política de segurança da informação explicita quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas, o que se constitui em um ponto forte em sua opinião; no entanto, o entrevistado SI, que deveria implementar estes controles nos sistemas, não tem conhecimento dos mesmos, considerando este um ponto fraco.

A segurança da informação participa do ciclo de vida dos sistemas através de validação de processos nas fases pré-desenvolvimentos e de auditorias nas aplicações nas fases de testes, conforme o testemunho de CSI, que considera este um ponto forte. O entrevistado SI confirma: “Até aonde tenho conhecimento, são compostos pareceres [pela Segurança da Informação] sob demanda dos coordenadores de projeto”. No entanto, o mesmo entrevistado considera este um ponto fraco pelo fato de ser, em sua opinião, uma ação reativa.

A instituição tem uma grande preocupação em avaliar as possíveis ameaças que cada sistema possa representar que considera esta avaliação um ponto forte, como ressalta CSI em seu comentário:

> Esta avaliação é feita antes da avaliação de segurança. Temos uma metodologia de gestão de projeto (PMI): uma das áreas é a análise de riscos; todos os riscos são mapeados no pré-projeto; é feita a avaliação, porque às vezes os riscos são tão grandes que inviabilizam o projeto. Isto é feito antecipando o projeto propriamente dito. Sendo aprovado o projeto, posteriormente há todo o acompanhamento da área de segurança. A TI faz e a Segurança acompanha (CSI).

Novamente discordante, o entrevistado SI alega ser ponto fraco, sendo esta uma ação reativa.

4.2.4 Segurança da Informação – Nível Operacional

O treinamento dos usuários finais no uso seguro dos sistemas é feito através de treinamentos presenciais e por treinamentos à distância com soluções de EAD. O entrevistado SI sintetiza, dizendo que os colaboradores recebem o treinamento e a conscientização habitual, em seu comentário:

> Anualmente: palestras anuais de conscientização. Na contratação de novos colaboradores (todos) tem um minitreinamento sobre segurança (aproximadamente 1 hora). Temos ferramentas de comunicação interna, o portal corporativo (comunicados, orientações, dicas, alertas), os murais (com cartazes), o site (mais voltado p/ o cliente) com a cartilha. Mas estamos num processo inicial de conscientização. Ainda não caiu a ficha da galera em relação a muita coisa. Senhas: uma base única de autenticação (LDAP), critérios de formatação de senhas bastante ‘chatos’. A política deixa claro que passar a senha p/ outros dá demissão, mas a gente sabe que tem gente que passa (CSI).

Este item foi considerado ponto forte pelos dois entrevistados.

Com vistas a esclarecer os clientes do banco sobre o uso seguro dos recursos de TI, são colocadas à sua disposição diversas ferramentas são utilizadas: o site institucional traz

informações sobre os recursos de segurança disponíveis para acesso ao *website*, ATM's e demais canais de relacionamento; existe um jornal bimestral que freqüentemente aborda o assunto, existem cartazes nas agências, e assim por diante. No entanto, CSI ressalta que,

> não temos nenhuma forma de *feedback* do cliente, para ver como ele se sente em relação à segurança. Ainda temos que evoluir. Estamos fazendo o nosso papel, tem informações no site, tem um jornalzinho (bimestral) que é enviado a praticamente todos os clientes [cerca de 1 milhão de exemplares], vou lá e escrevo alguma coisa sobre segurança. Sabemos que a informação chega até eles, mas não sabemos se eles estão lendo. Temos um *plug-in* no site (que deveria ser instalado no computador do cliente) que analisa o que está acontecendo; hoje o *plug-in* não é obrigatório, não sabemos se de fato é instalado. Mas nas próximas semanas a instalação do *plug-in* será obrigatória, como os outros bancos estão fazendo.

Mesmo com a ressalva de que não existe nenhuma forma de avaliar o nível real de consciência do cliente, os dois entrevistados consideram este um ponto forte.

A opinião dos clientes, entretanto, não demonstra tanto entusiasmo, como expressa CL1, ao dizer que,

> não lembro de ter sido esclarecido sobre isso [segurança da informação] e acho que este é um ponto fraco do banco. Por outro lado, creio que tal informação deve estar disponível, mas que obtê-la requeira que o cliente a procure, o que não é o padrão. O mesmo parece se aplicar a outros bancos.

A política de segurança da informação estabelece direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação. Segundo CSI, "este é o papel da política de segurança; é um ponto forte". O entrevistado SI, normalmente mais crítico, desta vez concorda, comentando que,

> a área de Risco Operacional e Segurança define especificamente quais os acessos de usuários e terceirizados, conforme a necessidade e o Regulamento de Segurança da Informação e os operacionaliza, quando necessário. Considero isso um ponto forte.

A documentação do projeto e da operação dos sistemas existe, mas nem sempre está atualizada. O entrevistado CSI relata que "A dinâmica das áreas de TI acaba limitando a atualização em 100% da documentação necessária", com o que SI concorda: "A

documentação dos sistemas de negócio, na maior parte das vezes, inexiste". Os dois entrevistados consideram este como sendo um ponto fraco.

Seguindo as boas práticas da norma ABNT ISO 17799:2005, a instituição financeira implementa critérios de aceitação para novos sistemas, atualizações e novas versões; são efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação. O entrevistado CSI vai mais longe, afirmando que "Existe uma metodologia de gerenciamento de mudanças, baseada em melhores práticas de gestão de infra-estrutura (ITIL) e desenvolvimento (CMMI) para atualizações na plataforma tecnológica". SI novamente concorda: "Há fluxos de desenvolvimento baseados no CMMI, desde o início do desenvolvimento das versões até a sua entrega e aceite final". Ambos consideram este como sendo um ponto forte.

Novamente apoiado na implementação da norma ABNT ISO 17799:2005, CSI diz que, "Existem controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança. Existem procedimentos para a devida conscientização dos usuários. É ponto forte." O entrevistado SI, novamente não se mostra tão otimista, ao afirmar que "Existem procedimentos de monitoramento isolados, que não abrangem ainda todos os sistemas. Há iniciativas nesse sentido. Considero um ponto fraco".

4.2.5 Segurança da Informação – Infra-estrutura

O processo de avaliação de tecnologias de infra-estrutura, no que diz respeito à segurança da informação, ocorre através de equipes multidisciplinares e metodologia de

gerenciamento de projetos para assertividade nas aquisições. A respeito de a infra-estrutura se constituir ou não em diferencial competitivo CSI, afirma que,

> concordo em parte com a afirmação de que infra-estrutura é diferencial competitivo. No caso dos bancos, não é *commodity*. Quanto mais dinheiro tem prá investir em TI, mais vai ganhar dinheiro. Não tenha dúvida disso. Trabalhamos em parceria com as áreas de TI.

A confiabilidade, segurança e estabilidade da infra-estrutura são consideradas ponto forte, para o entrevistado CSI, ao comentar que,

> sim, é confiável e segura. O nível de exigência é muito alto, se não fosse confiável seríamos cobrados de forma 'violenta'. É Banco Central, CVM, todo dia. Se o banco estiver fora do ar nos horários determinados p/ BACEN, está fora do mercado, fecha as portas. Não fez as transferências de reservas p/ o BACEN, não recebeu o *ok* do BACEN, está fora.

Já o entrevistado SI, muitas vezes crítico, afirma que "Parece-me que a infra-estrutura é consolidada o suficiente para garantir níveis mínimos de segurança".

Não há nenhum sistema de métricas formalizado para avaliar a qualidade da segurança da informação, no nível da infra-estrutura. No entanto, na opinião de CSI, a segurança é suficiente:

> Pelo volume relatado de incidentes, a segurança está boa. A única forma de avaliarmos são os incidentes. É óbvio que estão acontecendo coisas que não estamos pegando, que não são reportadas. Mas não há impactos grandes em relação a isto. Se tivesse um incidente muito grave em nível de infra-estrutura, haveria impacto financeiro, impacto de imagem, etc., isto não tem. Através da análise de incidentes periódicos se vê que estamos tendo efetividade. Mas não temos um sistema de gestão de infra-estrutura e gestão de incidentes (nos moldes do ITIL). Para gestão de incidentes de segurança, trabalhamos com planilha, com mapeamento de incidentes de forma manual. O processo já temos, já está mapeado, os subprocessos, está tudo mapeado e funcionando, só não tem nada automatizado, é tudo manual.

4.3 ESTUDO DE CASO 3

O Estudo de Caso 3 refere-se à instituição financeira pública de fomento, sem contas correntes, utilizada como estudo de caso contraste com as duas anteriores. As pessoas entrevistadas encontram-se relacionadas no Quadro 7.

Quadro 7
Entrevistados de EC3

Pessoa	Setor	Cargo/Função
CDT	Departamento de Tecnologia	Chefe do Departamento de Tecnologia
CSI	Departamento de Tecnologia	Coordenador de Segurança da Informação (este pesquisador)
CRO	Coordenadoria de Controles Internos e Risco Operacional	Coordenador de Controles Internos e Risco Operacional
CL1		Cliente institucional

4.3.1 Contexto Organizacional

Trata-se de uma instituição pública de fomento, conta com autonomia administrativa e personalidade jurídica próprias. As decisões são tomadas pela Diretoria (diretores nomeados politicamente).

Existe um Comitê de Gestão, composto por funcionários do quadro, subordinado à diretoria, que trata dos assuntos técnicos e administrativos, e os encaminha à diretoria para decisão. Não existe uma estrutura específica responsável pela segurança da informação; no entanto, há um analista de sistemas, vinculado ao Departamento de Tecnologia, responsável pela elaboração da Política de Segurança da Informação e da definição de *software* de

proteção e monitoramento necessários, bem como pelo estudo dos requisitos necessários para a implantação de um site redundante.

O Departamento de Tecnologia, responsável pela TI e pela segurança da informação, é vinculado à Superintendência de Infra-Estrutura, que por sua vez é vinculado à Diretoria Administrativa.

4.3.2 Segurança da Informação – Nível Estratégico

Não existe uma Política de Segurança da Informação formal. Existe uma regulamentação que abrange alguns pontos de uma política de segurança, como recomendações para senhas e regulamentação de uso da Internet e do correio eletrônico. Na opinião do entrevistado CDT, “Os níveis [de segurança] atualmente praticados são baixos, tanto pela falta de normas ou falta de formalização das mesmas, como também pela inexistência de ferramentas de controle”.

Segundo informações obtidas, está em discussão uma Política de Segurança da Informação cuja minuta prevê os 3 (três) níveis: estratégico, através de resoluções da diretoria; tático, através de instruções normativas de nível de superintendência, que implementem as resoluções, e normas específicas geradas a partir das instruções normativas, no nível operacional. Esta Política de Segurança da Informação é baseada na Norma ABNT ISO 17799:2005. Também está sendo discutida uma Política de Classificação da Informação, que a princípio terá 4 níveis: confidencial, restrita, interna e pública. O entrevistado CDT alerta que,

> o impacto que um problema de segurança da informação pode causar na estratégia competitiva pode ser grande, principalmente em termos de risco de reputação da instituição, algo que pode ser bastante difícil de recuperar. Além disso, a falta de disponibilidade de serviços por um tempo longo em relação às necessidades da instituição, pode trazer prejuízos financeiros para a mesma e mesmo implicar maior exposição a risco operacional.

No entanto, na opinião de CRO, os riscos não são tão grandes, conforme expressa:

> O impacto de uma quebra de confidencialidade das informações é baixo porque atuamos em nichos específicos; o impacto de uma alteração das informações é alto, devido ao risco legal e de imagem, e o impacto da indisponibilidade das informações é médio, dependendo do período de indisponibilidade.

No entanto, é forçoso observar que, diante da Lei Complementar nº 105/2001 ("Lei do Sigilo Bancário"), uma quebra de confidencialidade das informações (a qual pode facilmente redundar numa violação do sigilo de informações) é crime. Portanto, seu impacto é sempre alto.

O apoio da diretoria à segurança da informação tem se manifestado claramente. Recentemente foi designado um analista de sistemas para desenvolver e propor ao Comitê de Informática a política de Segurança da Informação. Isto pode ser visto pelo comentário entrevistado CDT ao expressar que:

> As ações devem ser propostas pelo quadro técnico. Tenho visto receptividade da Diretoria em atender às recomendações, desde que bem fundamentadas. O plano estratégico de TI para 2008 já foi aprovado. São dois grandes pontos a serem atacados – sistemas e segurança. Até o fim de 2008 a Política de Segurança da Informação, uma solução para continuidade e um plano de segurança precisam estar implantados.

O entrevistado CSI constata que "A diretoria, por ser política, delega ao Comitê de Gestão, a condução técnica e administrativa da instituição. Cabe aos técnicos sensibilizar e motivar o Comitê de Gestão, o qual deve discutir o assunto e leva-lo à diretoria". Porém, a opinião de CSI sobre a segurança da informação na instituição, expressa que ela:

> está restrita aos aspectos físicos (controle de acesso físico, *datacenter* climatizado, cópias de segurança em local remoto, contrato de manutenção de 4

> horas, etc.) e aspectos lógicos (*firewall*, antivírus, *software* de proteção, acesso integrado via LDAP, política de senhas, e assim por diante).

A partir da análise de documentos constata-se que a segurança da informação não contribui significativamente, neste momento, para garantir conformidade com padrões relevantes, regulamentações governamentais e contratos. Corroborando com esta observação, o entrevistado CDT diz que:

> Entendo que as normas consagradas de segurança da informação já possuem incorporadas boas práticas que as instituições devem utilizar. Adotar tais normas significa automaticamente aumentar o grau de conformidade com outras regulamentações. Atualmente, é ponto fraco.

Quando são formuladas novas estratégias organizacionais, não são considerados aspectos relacionados à TI nem à segurança da informação. Novamente a opinião de CDT vem ao encontro desta observação ao comentar que:

> Uma nova estratégia pode impactar processos e, em razão disso, o ambiente tecnológico necessário para suportar os mesmos, incluindo questões de segurança. Temos flexibilidade para atender uma mudança de estratégica? Acho que não, considerando portanto um ponto fraco.

Não há um ERP, o que existe são sistemas (*mainframe*: operações, financeiro, RH; plataforma baixa: Cadastro e Análise de Crédito, Contabilidade, Controle Patrimonial) que cumprem as funções operacionais da instituição. Segundo CDT, “Estes sistemas possuem algum grau de flexibilidade para novas demandas (não muito), mas há risco de alguma perda de segurança.” Existe ainda o *website* institucional, com o *Internet Banking* (restrito à emissão de boletos de pagamento). Porém a opinião de CRO expressa que ele acha “que [o *Internet Banking*] não suporta muito bem a segurança da informação porque tem problemas operacionais”.

4.3.3 Segurança da Informação – Nível Tático

Não há avaliação do desempenho da gestão da segurança da informação. O conceito de gestão de segurança da informação é incipiente na instituição, e inexiste uma estrutura formal responsável pelo assunto. CRO comenta que “Não temos procedimentos formais de Segurança da Informação”. Este é considerado ponto fraco pelos entrevistados.

As políticas específicas mais importantes são mostradas no Quadro 8, pela ordem de prioridade de citação.

Quadro 8
Principais Políticas de Segurança de Informação de EC3

Ordem	**Política de Segurança da Informação**	**Citação**
1	Conformidade com a legislação e cláusulas contratuais	CDT, CRO e CSI
2	Gestão da continuidade do negócio	CDT, CRO e CSI
3	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa	CDT e CSI
4	Detecção e prevenção de vírus e *software* malicioso	CRO
5	Conseqüências da violação da política de segurança	Não citado

Atualmente, pelo fato de não existir uma Política de Segurança da Informação institucionalizada, não são explicitados quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas. No entanto, observa-se que diversos controles e procedimentos (cópias de segurança (“*backup*”), segregação de ambientes para desenvolvimento e produção, rotinas de teste, controle de acesso ao banco de dados, restrições (“*constraints*”) no banco de dados, etc.) já são prática corrente ou estão em estágio avançado

de implantação. No documento que está em discussão este item é contemplado de forma explícita, englobando sugestões da norma ABNT ISO 17799:2005 e de mais algumas boas práticas coletadas em artigos científicos e livros técnicos. No atual estágio, no entanto, os entrevistados CDT, CRO e CSI consideram ponto fraco.

A partir da análise de documentos constata-se que a segurança da informação não participa do ciclo de vida dos sistemas, salvo em situações particulares. O entrevistado CDT concorda com esta visão ao afirmar que:

> A segurança da informação deveria fazer parte durante todo o ciclo. Cada sistema deve estar de acordo com controles e procedimentos de segurança definidos. Vale para o início do projeto, como também para as manutenções posteriores.

Concordando, CRO argumenta que "desde o projeto, durante o desenvolvimento, teste, implementação e suporte devem ser considerados os aspectos relacionados à Segurança da Informação". Há consenso quanto à problemática. Considerado ponto fraco por CDT, CRO e CSI. No entanto, de acordo com CSI, "no último ano muito foi feito, avançamos muito em relação ao final de 2006".

A análise de documentos e os depoimentos evidenciam que os projetos de TI não são avaliados para saber de que forma podem se constituir numa ameaça à segurança da informação. Considerado ponto fraco pelos entrevistados CDT, CRO e CSI. Novamente, a Política de Segurança da Informação em discussão abrange explicitamente este item, conforme explica o entrevistado CDT,

> temos problemas quando entra um sistema novo no ar. Não sabemos quais os requisitos. Colocamos no ar e pronto. A idéia é, neste momento, colocar uma pessoa vinculada à empresa terceirizada nesta função de discutir requisitos de infra-estrutura nos novos projetos.

4.3.4 Segurança da Informação – Nível Operacional

A análise dos documentos e as entrevistas demonstram que pouco tem sido feito no sentido de promover a consciência da segurança da informação. Todos os entrevistados internos consideram este um ponto fraco. Os usuários finais dos sistemas são treinados informalmente no uso seguro dos mesmos. Como comprovação desta falta de consciência, o entrevistado CRO expressa a seguinte opinião:

> Acredito que se os sistemas forem bem desenvolvidos, não haverá grandes riscos relacionados ao seu uso, de modo que o treinamento pode ser simplificado. Por exemplo, se houver bons software de *firewall* e *antispam*, serão menores os riscos de mau uso. Considero pouco relevante.

Por outro lado, tendo em mente o projeto de segurança em implantação, o entrevistado CDT observa que,

> em termos de comunicação, a Cartilha de Segurança da Informação deverá ser priorizada; deve ser simples, não 'chata de ler'. Depois entraremos com telas de fundo [relativas à segurança] como reforço. Faremos a Cartilha através de uma Resolução [da Diretoria]. A cartilha será parte do projeto de divulgação. A Assessoria de Comunicação deverá ser envolvida.

A consciência da segurança da informação por parte dos clientes não é crítica, por se tratar de instituição financeira de investimento, sem contas correntes movimentadas por internet, nem terminais de atendimento automático. Existe, no *website* do *Internet Banking*, um *link* com a Política de Segurança. Na opinião do entrevistado CRO, "Os clientes devem ser suficientemente esclarecidos para evitar risco de imagem". É considerado ponto fraco pelos entrevistados internos e pelo cliente entrevistado (CL1), que afirma: "Não sei se [a Política de Segurança] esclarece. Não conheço nada; se eles tivessem repassado alguma coisa relativa às suas políticas, eu saberia".

A análise dos documentos obtidos mostra que existe uma resolução da diretoria que estabelece regras para o uso da internet e do correio eletrônico; não há, no entanto, controle

sistemático sobre o uso. Como não existe Política de Segurança da Informação, não há estabelecimento formal de direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização. Mais uma vez, está previsto na política que está sendo discutida. Todos os entrevistados internos consideram este um ponto fraco.

A documentação dos sistemas existe parcialmente, nem sempre atualizada. Todos os entrevistados internos são unânimes em considerar este com um ponto fraco.

A análise da documentação e os depoimentos mostram que não existem critérios genéricos de aceitação para novos sistemas, atualizações e novas versões; no entanto, eles estão sendo implantados, com testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação. Em alguns sistemas mais sensíveis a problemas, esta sistemática já está em uso. Os entrevistados CDT e CSI consideram que este ainda deve ser considerado ponto fraco, embora este processo esteja em clara evolução.

A instituição não possui sistema formal de controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança. No entanto, como ressalva o entrevistado CSI,

> os sistemas do *mainframe*, onde estão os sistemas antigos, voltados ao negócio, funcionam de forma estável, sem maiores problemas de segurança. Os problemas se concentram na plataforma baixa, onde se constata um crescimento rápido e não planejado da infra-estrutura.

Os entrevistados CDT e CSI consideram que este é um ponto fraco na plataforma baixa, mas é ponto forte no *mainframe*, no qual são executados os sistemas críticos para o negócio.

4.3.5 Segurança da Informação – Infra-estrutura

As observações realizadas, bem como a análise da documentação e os depoimentos permitem concluir que a avaliação da plataforma baixa é feita informalmente. O entrevistado CDT corrobora esta observação: “Não há existência de um *checklist* contendo todos os aspectos a serem verificados”. No caso do *mainframe*, a avaliação é feita em conjunto por técnicos da empresa e do fornecedor. Nenhum dos entrevistados considera a infra-estrutura como sendo diferencial competitivo.

A confiabilidade da infra-estrutura, na avaliação de CDT, “é ponto fraco, pois, em parte, [a infra-estrutura] está desatualizada e requer otimização. A parte do *mainframe* tem se mostrado bastante confiável (*hardware*), mas não há contingência”.

Há relatos de problemas de indisponibilidade de sistemas e serviços, como correio eletrônico, servidor *http* de sistemas internos e problemas na administração da capacidade de discos. Concordando com o entrevistado CDT, CSI diz,

> a parte de *mainframe* está estável e funcionando; a parte de plataforma baixa está com problemas. Estamos providenciando um contrato de suporte (hoje é avulso), já licitamos a manutenção com 4 horas, precisamos de um *software* de monitoramento; temos dificuldade de colocar uma pessoa com conhecimentos específicos, em virtude de que não se pode contratar sem concurso e não se pode colocar pessoa terceirizada trabalhando diretamente no nosso ambiente.

Projeto em estudo prevê reformulação total na infra-estrutura; algumas ações já foram disparadas. Segundo CDT, “Estamos reestruturando os servidores, com idéia de virtualização”. A redundância de todos os servidores também está sendo discutida na agenda de 2008, já havendo previsão orçamentária.

Não há sistema formal de métricas de segurança da informação da infra-estrutura. Os entrevistados CDT, CRO e CSI são unânimes em considerar este um ponto fraco.

5 ANÁLISE DOS RESULTADOS

Neste capítulo encontra-se apresentada a análise dos resultados obtidos a partir dos estudos de casos. Foi empregado o *software* “Analisador Léxico”, citado no item 3.5, como ferramenta auxiliar para a determinação das categorias correspondentes a cada variável preliminar (Quadro 2), sendo estas correspondentes às palavras ou expressões mais freqüentes nas respostas relativas a cada questão do instrumento de pesquisa.

Após as análises, foi possível constatar como sendo um dos principais resultados desta pesquisa: “as instituições financeiras que possuem contas correntes (acessos on-line, de qualquer parte do mundo, durante as 24 horas do dia) são obrigadas a praticar padrões de segurança muito mais rígidos do que instituições financeiras que não possuam contas correntes”. As exigências do BACEN para estas instituições financeiras, bem como as ameaças via internet, conduziram para isto.

Os resultados a seguir encontram-se agrupados por nível de segurança da informação (estratégico, tático e operacional) da seguinte forma: primeiro, foi realizada uma análise sintética e foram agrupados os resultados encontrados para os estudos de caso 1 e 2 (instituições financeiras com contas correntes); segundo, foi realizada uma análise sintética para os resultados obtidos no estudo de caso 3 (instituição financeira de fomento); e, por último, para efeitos de contraste, os resultados agrupados dos estudos de caso 1 e 2 foram comparados com os resultados do estudo de caso 3. Por fim, foi realizada uma convergência dos elementos resultantes da observação prática com os elementos propostos no Modelo Preliminar para Estudo (Figura 2).

5.1 CONVERGÊNCIA DOS RESULTADOS AGRUPADOS ENTRE OS CASOS 1 E 2

Nesta seção foi realizada a convergência das principais características resultantes da análise dos estudos de caso 1 e 2, ambas as instituições financeiras com conta corrente. A análise foi estruturada da seguinte forma: observou-se o *framework* (modelo ou padrão) de segurança da informação utilizado, as variáveis promotoras de alinhamento em nível estratégico, em nível tático e em nível operacional e, as variáveis de infra-estrutura de maior ocorrência. Por fim, os principais elementos que levam ao modelo de pesquisa estudado (Figura 2).

As semelhanças constatadas entre os casos 1 e 2 relativas aos *frameworks* utilizados são as seguintes:

- Padrão de auditoria do BACEN: COBIT (para maiores explicações ver item 2.2.3.1 COBIT);

- Padrão de governança de TI: ITIL (para maiores explicações ver item 2.2.3.2 ITIL);

- Padrão de projetos de TI: CMMI (*Capability Maturity Model Integration*, ou integração dos modelos de maturidade da capacidade - é um modelo de qualidade, abrangendo 5 fases: inicial, gerenciado, definido, quantitativamento gerenciado e em otimização);

- Padrão de segurança da informação: ABNT ISO 17799:2005 (para maior detalhamento ver item 2.3.2 A Norma ISO/IEC 17799).

Conforme a literatura, os *frameworks* de auditoria (COBIT), governança de TI (ITIL) e segurança da informação (ABNT ISO 17799:2005) empregados pelas instituições financeiras dos casos 1 e 2 são largamente utilizados, sendo inclusive recomendado o seu uso conjunto (OGC, 2007; BERNARDES e MOREIRA, 2005; ITGI, 2005).

5.1.1 Convergência das variáveis no Nível Estratégico

O resultado do agrupamento dos elementos e variáveis promotores de alinhamento estratégico entre as políticas de segurança de informação e as estratégias e práticas adotadas pela TI encontradas em ambos os estudos de casos (1 e 2), no **nível estratégico** foram as seguintes: níveis de segurança, impacto no negócio, apoio da diretoria, conformidade, efeitos da estratégia na TI, e ferramenta estratégica.

Com relação à variável “níveis de segurança”, foi possível constatar que tanto EC1 quanto EC2 possuem uma Política de Segurança da Informação formalizada, abrangendo os 3 níveis. As nomenclaturas utilizadas são diferentes entre as instituições, mas existem diretrizes (no nível estratégico), normas (no nível tático) e procedimentos (no nível operacional), de forma similar ao modelo citado por Oliva (2003), o qual classifica uma política de segurança da informação em 3 níveis: diretrizes, normas e procedimentos.

Para ambos os casos a variável “impacto no negócio” mostrou que qualquer impacto relativo à quebra de segurança é crítico no negócio. A quebra de confidencialidade das informações pode resultar num grande impacto para a imagem pública da empresa; a alteração indevida de informações pode implicar a perda de credibilidade da instituição diante de seus clientes; a indisponibilidade das informações certamente resultará na perda de negócios, em

especial, o *homebanking-officebanking* e o comércio eletrônico, e igualmente em dano severo à imagem. No ambiente bancário impera a Lei Complementar nº 105/2001 (Lei do Sigilo Bancário), o que requer um tratamento adequado do cadastro de clientes de instituições financeiras e dos seus dados financeiros. Quebra de confidencialidade é crime.

Com relação à variável "apoio da diretoria" para ambos os casos, o apoio da Diretoria à Segurança da Informação é claro e explícito, tendo ambas as diretorias tomado iniciativas concretas para tais políticas, dando prioridade para os projetos que envolvem segurança. O *software* "Analisador Léxico" relacionou como candidata a nova categoria a expressão "estruturas específicas", pois nos dois casos, foram criadas estruturas específicas para a Segurança da Informação, jamais subordinadas à TI; pelo contrário, são estruturas do mesmo nível hierárquico que a TI, subordinadas diretamente à Diretoria. Esta disposição hierárquica corrobora a idéia de Lessa (2006) sobre a liderança do projeto de segurança da informação por um executivo que não pertença à área de TI, ou seja, a separação das áreas de TI e de Segurança da Informação. Este aspecto resultante também pode ser reforçado pela posição de um dos entrevistados, quando cita que:

> O processo de tirar a segurança de dentro da TI é um processo migratório pelo qual todos os bancos já passaram – da segurança nascer dentro da TI e migrar para um nível superior. É o cenário ideal. Nos grandes bancos a Segurança da Informação já saiu debaixo da Diretoria de TI. O ideal é haver uma Diretoria de Segurança ou de Risco, independente da TI. Quem estabelece políticas de segurança e vai auditar outras áreas não pode estar subordinado hierarquicamente. Desvincular a Segurança da Informação da TI é fator crítico de sucesso.

Os resultados encontrados nos casos estudados também são reforçados através dos resultados expressos pela literatura e pela norma ABNT ISO 17799:2005 como aspectos críticos, ou seja, de que "a diretoria deve estabelecer uma clara orientação da política, alinhada com os objetivos do negócio e demonstrar apoio e comprometimento com a

segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização".

A variável "conformidade" (com leis, regulamentos e contratos), para ambos os casos, também se mostrou crítica. O esforço feito por todo o sistema bancário brasileiro para alcançar a conformidade com as resoluções do BACEN, especialmente a Resolução 3.380 ("Risco Operacional"), é digno de nota. Isto é demonstrado também na opinião de um dos entrevistados quando cita que "alinhamento da Resolução 3380 do BACEN (Basiléia II) como prioridade das ações da estratégia do Banco"; "a Resolução 3380 possui várias frentes; a frente de Segurança, que atinge toda a parte de informática, está dentro da Segurança de TI". É ponto forte. Portanto, foi possível constatar o que é recomendado pela norma ABNT ISO 17799:2005 nas duas instituições: "A política de segurança da informação objetiva prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações pertinentes".

Para ambos os casos, a variável "efeitos da estratégia na TI", mostrou que sempre há um risco de que a formulação de uma nova estratégia organizacional afete a TI e a segurança da informação. A formulação de novas estratégias deve levar em consideração a segurança da informação ou, na opinião de um dos entrevistados, "deve estar alinhada com a segurança da informação e a TI". Existe a consciência da necessidade de se levar a segurança em consideração; é ponto forte. Estes resultados convergem com a proposta de modelo de alinhamento da TI com a política de segurança da informação de Doherty e Fulford (2005a), segundo a qual, após a equipe de estratégia ter conduzido a análise da situação e formulado uma estratégia, seu impacto na política de segurança da informação deverá ser revisto, e a política de segurança modificada, se for o caso, com vistas a adquirir conformidade com a nova estratégia.

A variável “ferramenta estratégica” também foi similar em ambas as instituições, através de *software* similares como Sistema de Gestão (ERP) e Site institucional/*Internet Banking*. Uma das instituições indicou a existência de um Sistema de Informação Executiva (EIS), que dificilmente a outra não utilizaria, apesar de não ter sido relacionado. Por outro lado, esta outra instituição possui um sistema de Sistema de Relacionamento (CRM). Nenhum entrevistado conseguiu relatar como cada um deles dá suporte à estratégia competitiva da empresa nem como cada um deles suporta a segurança da informação.

Em virtude das respostas evasivas e pouco esclarecedoras, fica difícil confirmar a afirmação de Oliva (2003), de que as organizações utilizam diversos sistemas informatizados que fornecem as informações necessárias para a definição de cenários e para a tomada de decisão, como ferramentas para a implantação da estratégia competitiva. No entanto, a análise visual dos *websites* das duas instituições torna claro que estes são ferramentas para a implantação das respectivas estratégias competitivas.

5.1.2 Convergência das variáveis no Nível Tático

O resultado do agrupamento dos elementos e variáveis promotores de alinhamento estratégico entre as políticas de segurança de informação e as estratégias e práticas adotadas pela TI encontradas em ambos os estudos de casos (1 e 2), em **nível tático** foram as seguintes: sistema de medição, políticas específicas, controles de segurança, ciclo de vida dos sistemas, e projetos de TI como ameaça.

Quanto à variável “sistema de medição”, faz-se necessário esclarecer que a avaliação que uma empresa faz da segurança da informação (ou seja, as métricas utilizadas) não diz

respeito, neste nível, a avaliações sobre desempenho, disponibilidade e confiabilidade da infra-estrutura; diz respeito a como a empresa avalia a adequação das normas de segurança da informação às estratégias empresariais e regulamentações pertinentes. Um dos critérios adotados é a avaliação de incidentes (quantitativa e qualitativamente). São avaliadas perdas financeiras evitadas, confrontando com situações anteriores. Auditorias externas são muito empregadas em bancos para avaliação da segurança, em todos os níveis. Uma medida num dos bancos é o prestígio junto à diretoria e aos colegas. Medidas comentadas na literatura, tais como ROI (*Return on Investment*) e outras, não são citadas, embora haja uma tentativa de quantificação de retorno em termos de danos evitados. Nos dois casos (EC1 e EC2) é considerado ponto forte, de forma quase unânime.

Embora não haja, nos dois casos estudados, um sistema formalizado de avaliação do desempenho da segurança da informação, existe de fato uma avaliação que, conforme preconiza a norma ABNT ISO 17799:2005, “seja usada para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria”.

De uma forma geral, os dois bancos têm visão semelhante a respeito da variável “políticas específicas”; ambos concordando com a ordem de importância das mesmas, conforme apresentado no Quadro 9.

Considerando o peso que a fiscalização do BACEN tem sobre os bancos, não há surpresa ao percebermos que a política mais importante é a conformidade com a legislação e cláusulas contratuais (ou seja, principalmente com as resoluções do próprio BACEN), e em segundo lugar a gestão da continuidade do negócio, exigência da Resolução 3.380 do BACEN.

Quadro 9
Principais Políticas de Segurança de Informação

Ordem	Política de Segurança da Informação
1	Conformidade com a legislação e cláusulas contratuais
2	Gestão da continuidade do negócio
3	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa

Merece comentário o item “Detecção e prevenção de vírus e software malicioso”, não citado no Quadro 9. Nenhum computador, nem mesmo de uso doméstico, pode funcionar sem ter pelo menos *software* antivírus instalado. Não há necessidade de política de segurança, um computador simplesmente não funciona sem este tipo de *software*. Então este item passa a perder importância quando se fala de alinhamento estratégico, porque é condição *sine qua non* para o funcionamento de qualquer computador, nos dias de hoje. Desta forma, novamente encontram-se satisfeitos os requisitos da ABNT ISO 17799:2005, a qual recomenda:

> A adoção de políticas específicas, que devem abranger política de segurança organizacional, política de classificação e controle de ativos da informação, política de segurança em pessoas, política de segurança física e do ambiente, política de gerenciamento das operações e comunicações, política de controle de acesso, política de desenvolvimento e manutenção de sistemas, política de gestão de continuidade de negócio e política de continuidade.

A variável “controles de segurança” também foi similar em ambas as instituições. Nos dois casos, a política de segurança da informação explicita quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas de forma genérica. Os controles e procedimentos são estabelecidos nas normativas específicas ou nos manuais dos respectivos sistemas.

No entanto, em um dos bancos aparece uma opinião contrária: um respondente alega que a TI não tem conhecimento, ou tem conhecimento insuficiente, destes controles e procedimentos. Com a exceção deste respondente, os demais consideram como sendo um ponto forte, o que parece indicar que a política de segurança da informação explicita quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas, mas que pode estar ocorrendo um problema de comunicação, que impeça o efetivo conhecimento, e por decorrência a aplicação, destas especificações na construção dos (ou de alguns) sistemas.

Assim, nos casos dos dois bancos, é obedecido o requisito da ABNT ISO 17799:2005, no sentido de que “devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhoria nos existentes”, embora pareça haver dúvidas sobre sua correta divulgação em pelo menos um dos casos.

A variável “ciclo de vida dos sistemas**”**, da mesma forma, encontra implementação semelhante nos dois casos. Em ambos os bancos, a segurança da informação participa do ciclo de vida dos sistemas através de validação de processos nas fases pré-desenvolvimentos e de auditorias nas aplicações nas fases de testes. Participa em todo o ciclo, desde a fase de planejamento até a operação, visando minimizar riscos de falhas. Parece ser ponto forte.

Foi possível verificar para ambos os casos, a exigência “as organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas” citada nas pesquisas de Bernardes e Moreira (2005).

A variável “projetos de TI como ameaça”, nos dois bancos, é tratada de forma similar, sendo feita a avaliação de como cada sistema pode se constituir num risco à segurança. Nos

dois casos, os respondentes ligados à coordenação da segurança da informação consideram este um ponto forte. No entanto, um analisa de sistemas de um banco e um analista de segurança do outro não concordam, utilizando, respectivamente, os seguintes argumentos: “Considero um ponto fraco pelo fato de ser uma ação reativa” e “Esta avaliação ainda não está sendo feita de forma conjunta entre área gestora do sistema, auditoria e segurança. A princípio, somente a área gestora do sistema faz uma avaliação individualizada. Não considero um ponto forte”.

Uma forma de evitar que um projeto de TI se constitua numa ameaça à segurança da informação, é providenciar para que cada projeto de TI, documentado no PESI, seja avaliado criticamente para identificar as possíveis ameaças que representa, como preconizam Doherty e Fulford (2005a). De posse desta lista de possíveis ameaças, a política de segurança existente deverá ser revisada e eventualmente modificada. Percebe-se que os dois bancos estudados têm clara esta preocupação, mas fica claro que a implementação ainda não permite dizer que a condição seja satisfeita; parece ainda carecer de um maior amadurecimento.

5.1.3 Convergência das variáveis no Nível Operacional

O resultado do agrupamento dos elementos e variáveis promotores de alinhamento estratégico entre as políticas de segurança de informação e as estratégias e práticas adotadas pela TI encontradas em ambos os estudos de casos (1 e 2), em **nível operacional** foram as seguintes: consciência da segurança da informação (usuários finais dos sistemas), consciência da segurança da informação (clientes), relacionamento com usuários, documentação, critérios de aceitação, e controles.

Com relação à variável “consciência da segurança da informação (usuários finais dos sistemas)”, percebe-se, em ambos os casos, um esforço considerável no sentido de treinar adequadamente os usuários finais sobre segurança da informação e no uso seguro dos sistemas. Foi possível constatar isto através de atitudes típicas como a divulgação da Política de Segurança, treinamentos específicos, palestras internas e externas e campanhas mercadológicas de segurança, treinamentos a distância. Todos os entrevistados consideram este um ponto forte.

Em ambos os casos, foi possível constatar um grande esforço no sentido da implantação de uma “consciência da segurança da informação”, variável esta levantada por diversos autores, entre eles Kruger e Kearney (2006).

Com relação à variável “consciência da segurança da informação (clientes), a disponibilização de informações nos *websites* dos bancos sobre segurança da informação aos usuários é prática comum. Dos 15 principais bancos com atuação no Brasil, apenas 6 (seis) não disponibilizam aos seus usuários um *link* sobre ”Segurança”, “Política de Segurança” ou “Segurança da Informação” na primeira página do seu site, de forma facilmente localizável conforme apresentado no Quadro 10 (FINANCENTER, 2007).

A questão da conscientização dos usuários é um problema sério, pois não depende apenas do esforço dos bancos. Nos dois casos estudados, os respectivos *websites* contém *links* sobre “Segurança”, “Política de Segurança” ou “Segurança da Informação” na primeira página, com bastante material, em linguagem acessível ao usuário comum (desde que acostumado ao uso de computador).

Quadro 10
Bancos com *websites* com link para Segurança da Informação

	Banco	Dicas de segurança
1	Banco do Brasil	Sim
2	Caixa Econômica Federal	Sim
3	Bradesco	Sim
4	Itaú	Sim
5	Real - ABN AMRO	Não
6	HSBC	Sim
7	Unibanco	Sim
8	Santander Banespa	Sim
9	Nossa Caixa	Sim
10	Votorantim	Não
11	Safra	Não
12	Banrisul	Sim
13	Citibank	Não
14	UBS Pactual	Não
15	BNP Paribas	Não

(Fonte: http://financenter.terra.com.br/Index.cfm/Fuseaction/Secao/Id_Secao/462)

Além do *website*, são utilizadas campanhas de *marketing*, *folders* e cartazes, artigos em revistas internas, palestras externas. Adicionalmente, os dois bancos pesquisados disponibilizam diversos mecanismos de segurança nas respectivas páginas de *internet banking*, como a instalação de um *plug-in* para maior segurança das transações bancárias. As pessoas entrevistadas, funcionários dos bancos, consideram, sem dúvida, um ponto forte, embora em alguns casos, tivessem consciência de que não existe nenhuma forma de *feedback* do cliente, para ver como ele se sente em relação à segurança. Ainda existe a necessidade de evoluir. Em relação aos clientes consultados, não há unanimidade. Nenhum cliente revelou ter lido e seguido as instruções constantes nos *websites*; de uma forma geral, os clientes demonstram desconhecer a política de segurança publicada pelos seus bancos.

A importância do esclarecimento dos usuários dos bancos a respeito da segurança da informação é corroborada por Jorge Krug, Superintendente de Segurança da Informação do BANRISUL, em entrevista ao *website* BAGUETE (2006):

> O sujeito da proteção de dados deve ser sempre o usuário, e não a empresa. Especialmente no meio bancário. Em bancos o cliente precisa estar seguro o tempo todo. A instituição não pode prestar atenção somente à segurança interna, pois, ao oferecer algo como *internet banking*, por exemplo, estará possibilitando uma operação sua a ser executada em ambiente alheio – o local de onde o usuário acessará o serviço. Se alguma fraude ocorrer à conta do cliente, quem arcará com o prejuízo certamente será a instituição. Há diversas formas de fornecer esta proteção ampla. Por exemplo, garantindo a segurança do sistema de *home banking* como um todo e orientando os clientes quanto a formas corretas de utilização de sua conta on-line.

Assim como Guilherme Lessa, Diretor de TI do Banco Matone, na mesma entrevista, complementa dizendo que:

> Não só o usuário, como também o pessoal da empresa deve ser orientado. Não adianta investir em *firewalls*, antivírus e outras tantas ferramentas afins se a equipe não estiver apta a operar e entender estes recursos (BAGUETE, 2006).

Em outra entrevista mais recente, concedida ao mesmo órgão de imprensa (BAGUETE, 2007), Guilherme Lessa, perguntado sobre qual seria a maior preocupação do setor bancário em relação à área de segurança, respondeu:

> O usuário, que tem uma certa ingenuidade no uso de ferramentas bancárias na Internet, por exemplo, ou em terminais eletrônicos. Para o criminoso, é muito mais fácil fraudar uma conta individual do que toda a fortaleza que é o sistema – ou os sistemas – de um banco. Assim, é preciso que as pessoas tomem cuidado, se informem sobre formas de proteção de suas informações e se acostumem a não disseminar seus hábitos e dados pessoais em sites comumente utilizados para extração ou 'roubo' destes conteúdos, como *Orkut*, MSN e *Second Life*. Todos estes serviços, como qualquer um de seus similares, têm risco associado.

Este parece ser um ponto crítico, pois os bancos pesquisados colocam as informações à disposição dos seus clientes por vários meios (*websites*, cartazes, panfletos, material publicitário, etc.), e não há indício de que os clientes de fato se apropriem deste conhecimento. Se existe uma boa consciência no meio dos usuários finais (empregados e colaboradores em geral), o mesmo não se pode dizer em relação aos clientes. Apesar da realização, em ambos os casos, de um grande esforço no sentido da implantação de uma "consciência da segurança da informação", como apontado por Kruger e Kearney (2006), não se pode dizer que, de fato, esta consciência exista entre os clientes.

A variável “relacionamento com usuários” encontra similaridade nos dois casos, nos quais as respectivas políticas de segurança da informação estabelecem direitos e responsabilidades, inclusive limites a terceirizados e estagiários. Existem instrumentos como termo de compromisso para o uso de sistemas, informações e recursos de TI da empresa. Considerado ponto forte pelos entrevistados.

Portanto, em ambos os casos é seguida a norma ABNT ISO 17799:2005, onde está descrito que a política de segurança da informação deve estabelecer direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização; o relacionamento com os usuários precisa ser claro e bem definido.

A variável “documentação” não foi expressa de maneira significativa e positiva nos dois casos estudados: a documentação do projeto e da operação dos sistemas existe, mas nem sempre está atualizada. A dinâmica das áreas de TI acaba limitando a atualização em 100% da documentação necessária. É ponto fraco na opinião dos entrevistados. Portanto, não se verifica o que é preconizado por O’Brien (2001), de que documentação do projeto dos sistemas e *software* e a operação do sistema devem ser desenvolvidos e mantidos atualizados.

A variável “critérios de aceitação”, por sua vez, pode ser considerada ponto forte nos dois bancos. Para ambos os casos existe um ambiente específico de desenvolvimento de sistemas (o que é uma das boas práticas apontadas pela ABNT ISO 17799:2005). Assim, é satisfeita a boa prática proposta pela norma ABNT ISO 17799:2005:

> Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e devem ser efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.

Ademais, o *software* “Analisador Léxico” relacionou como candidata a nova categoria a expressão “ITIL”; existe, nos casos EC1 e EC2, uma metodologia de gerenciamento de mudanças, baseada em melhores práticas de gestão de infra-estrutura (ITIL).

Nos dois casos, a variável “controles” encontra-se implementada: existem controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança (detecção de invasão, antivírus, *antispam* e assemelhados). Por unanimidade, considerado ponto forte no que diz respeito a controles. No entanto, a questão dos procedimentos parece não estar bem resolvida. Há procedimentos de monitoramento isolados, que não abrangem ainda todos os sistemas. Embora a situação esteja em evolução, é ponto fraco.

A norma ABNT ISO 17799:2005 diz que devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários. Há controles que atendam à norma, os procedimentos carecem de maior amadurecimento.

5.1.4 Convergência das variáveis da Infra-estrutura

O resultado do agrupamento dos elementos e variáveis promotores de alinhamento estratégico entre as políticas de segurança de informação e as estratégias e práticas adotadas pela TI encontradas em ambos os estudos de casos (1 e 2) da **infra-estrutura** foram as seguintes: diferencial competitivo, confiabilidade, e métricas.

A variável “diferencial competitivo” estabelece se a infra-estrutura representa ou não diferencial competitivo. A avaliação de novas tecnologias de infra-estrutura, no que diz

respeito à segurança da informação, é feita em laboratório ou ambiente de homologação, por equipes multidisciplinares e com metodologia de gerenciamento de projetos. Um dos entrevistados diz que a área de Segurança não define tecnologia, só estabelece princípios. Não há referências a ser um diferencial competitivo, embora outro entrevistado assim considere.

Desta forma, fortalece-se a afirmação de Davenport (1998) de que, embora o funcionamento correto e adequado desta infra-estrutura seja crítico, a aquisição de tecnologias infra-estruturais raramente significa uma vantagem competitiva em si. O que é vantagem competitiva não é a infra-estrutura propriamente dita, mas sim os projetos que ela suporta.

No caso da variável “confiabilidade”, novamente há convergência entre os dois casos estudados. A confiabilidade, segurança e estabilidade da infra-estrutura dos dois bancos são consideradas ponto forte, pois qualquer tipo de instabilidade, falta de segurança ou perda da confiabilidade, afetará toda a empresa e conseqüentemente a sua imagem pública. Além deste prejuízo, também poderá gerar um prejuízo financeiro.

Embora a infra-estrutura não seja diferencial competitivo, para Bernardes e Moreira (2005), o crescimento e o sucesso das organizações, atualmente, estão diretamente relacionados à necessidade de se manter uma infra-estrutura de TI segura e confiável, o que foi possível verificar nos dois casos estudados.

A variável “métricas” também se encontra implementada nos dois casos, onde métricas em nível de infra-estrutura são praticadas normalmente. Isto está de acordo com o assunto do debate promovido pelo Baguete Diário, em 26 de setembro de 2006, reunindo, Jorge Krug (CSO do Banrisul), Guilherme Lessa (Diretor Administrativo e de TI do Grupo Matone) e Fábio Ramos (Diretor da Axur Information Security) onde a importância de um

sistema de métricas para monitorar a segurança da informação foi destacada (BAGUETE, 2006).

Quando entrevistado pro telefone, Fábio Ramos expressa que,

> Segurança por segurança não vale nada. É preciso controlar o processo, pois, sem controle, não posso medir e, sem medir, não posso gerenciar. É preciso gerir a escolha e implantação das ferramentas adotadas, para que se alinhem à política de negócios de cada organização.

Desta foram, em ambos os casos, foram atendidos os requisitos da ABNT ISO 17799:2005:

> As redes devem ser adequadamente gerenciadas e controladas, de forma a serem protegidas contra ameaças; deve ser mantida a segurança de sistemas que utilizam estas redes, incluindo a informação em trânsito.

5.1.5 Convergências gerais entre os elementos dos Casos 1 e 2 e da literatura

Os principais elementos encontrados resultantes da convergência dos dados coletados e analisados dos casos e aqueles identificados na literatura encontram-se apresentados no Quadro 11. Não foi possível constatar diferença significativa em relação às variáveis identificadas para as duas instituições financeiras estudadas (casos 1 e 2). Constatou-se que os resultados agrupados atendem plenamente a 13 variáveis encontradas na literatura, parcialmente 6 variáveis e não atende a 1 variável.

Na dimensão “Negócio”, elemento “Nível Estratégico”, a variável “níveis de segurança” é plenamente atendida nos dois estudos de caso, ou seja, as respectivas políticas de segurança da informação são constituídas em 3 níveis (estratégico, tático e operacional; a variável “impacto no negócio” é plenamente atendida, à medida que, de fato, qualquer quebra

de confidencialidade, integridade ou disponibilidade das informações pode acarretar impactos profundos no negócio; a variável “apoio da diretoria” é plenamente atendida, pois ambas as diretorias têm apoiado decisivamente a segurança da informação, inclusive com a criação de estruturas de nível de superintendência para tratar especificamente do assunto.

Quadro 11
Comparação das Dimensões, Elementos e Variáveis dos Casos 1 e 2 com as Variáveis do Modelo Preliminar

Dimensões	Elementos	Variáveis Preliminares	Atendimento com literatura
Negócio	Nível Estratégico	Níveis de segurança	Plenamente atendido
		Impacto no negócio	Plenamente atendido
		Apoio da diretoria	Plenamente atendido
TI	Nível Estratégico	Conformidade	Plenamente atendido
		Efeitos da estratégia na TI	Plenamente atendido
		Ferramenta estratégica	Parcialmente atendido (somente *websites*)
Negócio	Nível Tático	Sistema de medição	Parcialmente atendido (não há medidas formais)
		Políticas específicas	Plenamente atendido
TI	Nível Tático	Controles de segurança	Parcialmente atendido (há dúvidas sobre a divulgação dos controles)
		Ciclo de vida dos sistemas	Plenamente atendido
		Projetos de TI como ameaça	Parcialmente atendido (processo carece de amadurecimento)
Negócio	Nível Operacional	Consciência da segurança da informação (usuário dos sistemas)	Plenamente atendido
		Consciência da segurança da informação (cliente)	Parcialmente atendido (não há *feedback* sobre a consciência do
		Relacionamento com usuários	Plenamente atendido
TI	Nível Operacional	Documentação	Não atendido (documentações inexistentes ou desatualizadas)
		Critérios de aceitação	Plenamente atendido
		Controles	Parcialmente atendido (existem controles; procedimentos carecem de amadurecimento)
Negócio & TI	Infra-Estrutura	Diferencial competitivo	Plenamente atendido (não é diferencial competitivo)
		Confiabilidade	Plenamente atendido
		Métricas	Plenamente atendido

Na dimensão “TI”, elemento “Nível Estratégico”, a variável “conformidade” é plenamente atendida, principalmente em função do esforço feito por todo o sistema bancário brasileiro para alcançar a conformidade com as resoluções do BACEN, em especial a Resolução 3.380 (“Risco Operacional”); a variável “efeitos da estratégia na TI” é plenamente atendida, pois existe a consciência da necessidade de se levar a TI e a segurança em consideração na formulação de novas estratégias organizacionais; a variável “ferramenta estratégica” é apenas parcialmente atendida, graças a respostas evasivas e pouco esclarecedoras por parte dos entrevistados. No entanto, a análise visual dos *websites* das duas instituições torna claro que estes são ferramentas para a implantação das respectivas estratégias competitivas.

Na dimensão “Negócio”, elemento “Nível Tático”, a variável “sistema de medição” é parcialmente atendida, pois não há medidas formais; no entanto, existem diversas formas de avaliação que as empresas fazem da segurança da informação; a variável “políticas específicas” é plenamente atendida, pois as políticas satisfazem um dos requisitos da ABNT ISO 17799:2005.

Na dimensão “TI”, elemento “Nível Tático”, a variável “controles de segurança” é parcialmente atendida, pelo fato de ambas as empresas possuírem controles, mas haver dúvidas sobre a sua correta divulgação; a variável “ciclo de vida dos sistemas” é plenamente atendida, pois a segurança da informação participa do ciclo de vida dos sistemas através de validação de processos nas fases pré-desenvolvimentos e de auditorias nas aplicações nas fases de testes; a variável “projetos de TI como ameaça” é parcialmente atendida, em ambos os casos, porque existe a preocupação de encarar os projetos de TI como ameaças, mas o processo carece de amadurecimento.

Na dimensão “Negócio”, elemento “Nível Operacional”, a variável “consciência da segurança da informação (usuário dos sistemas)” é plenamente atendida nos dois casos, pois há diversas iniciativas neste sentido; a variável “consciência da segurança da informação (cliente)” é parcialmente atendida pois, apesar do esforço das duas instituições bancárias, não há *feedback* sobre a real consciência do cliente; a variável “relacionamento com usuários” é plenamente atendida porque as respectivas políticas de segurança da informação estabelecem direitos e responsabilidades, inclusive limites a terceirizados e estagiários.

Na dimensão “TI”, elemento “Nível Operacional”, a variável “documentação” não é atendida: as documentações são muitas vezes desatualizadas, e por vezes não existem; a variável “critérios de aceitação” é plenamente atendida, pois são implementadas as boas práticas recomendadas pela ABNT ISO 17799:2005 relativas à segregação de ambientes de desenvolvimento e produção, existem rotinas de teste documentadas, e assim por diante; a variável “controles” é parcialmente atendida, porque os controles existem, mas os procedimentos carecem de amadurecimento, em ambos os casos.

No elemento “infra-estrutura”, a variável “diferencial competitivo” é atendida, à medida que a infra-estrutura não pode realmente ser considerada como diferencial competitivo; a variável “confiabilidade” é plenamente atendida; a confiabilidade da infra-estrutura é absolutamente crítica para instituições financeiras que possuam qualquer tipo de acesso *on-line*; finalmente, a variável “métricas” é plenamente atendida, porque as métricas de nível de infra-estrutura são praticadas normalmente nas duas empresas.

5.2 ANÁLISE SINTÉTICA DOS PRINCIPAIS RESULTADOS DO CASO 3

O caso EC3 diz respeito à instituição financeira de fomento, que não possui contas correntes nem transações *on-line*. Ele foi utilizado como contraste entre os dois casos anteriores no intuito de reforçar os resultados e o modelo final encontrados. Vale lembrar que o pesquisador é um dos responsáveis pela segurança de informação desta instituição atuando tanto em nível estratégico como tático, operacional e em infra-estrutura. Isto vem reforçar a representatividade dos resultados aqui encontrados. No entanto, visando reduzir o viés de interpretação, o pesquisador buscou confirmar suas percepções com os demais envolvidos no projeto.

Os *frameworks* utilizados por esta empresa são as seguintes:

- Padrão de auditoria do BACEN: COBIT (para maiores explicações ver item 2.1.3.1 COBIT). No caso desta instituição financeira, pelo fato de não existirem contas correntes nem acessos *on-line*, a auditoria do BACEN é feita de forma bastante diferenciada;

- Padrão de governança de TI: não existe; há planos para a implantação do ITIL (para maiores explicações ver item 2.1.3.2 ITIL);

- Padrão de projetos de TI: não existe; há planos para a implantação do CMMI (*Capability Maturity Model Integration*, ou integração dos modelos de maturidade da capacidade - é um modelo de qualidade, abrangendo 5 fases: inicial, gerenciado, definido, quantitativamento gerenciado e em otimização);

- Padrão de segurança da informação: diversas práticas são baseadas na ABNT ISO 17799:2005, mas não existe política de segurança da informação formalizada. A política que está sendo implementada se baseia na supracitada norma ABNT (para maior detalhamento ver item 2.3.2 A Norma ISO/IEC 17799).

Conforme a literatura, os *frameworks* de auditoria (COBIT), governança de TI (ITIL) e segurança da informação (ABNT ISO 17799:2005) que estão em implantação (ou que a instituição pretende implantar) são largamente utilizados, sendo inclusive recomendado o seu uso conjunto (OGC, 2007; BERNARDES e MOREIRA, 2005; ITGI, 2005).

5.2.1 Variáveis do Elemento Promotor de Alinhamento – Nível Estratégico

As varáveis do elemento promotor de alinhamento **nível estratégico** são as seguintes: níveis de segurança, impacto no negócio, apoio da diretoria, conformidade, efeitos da estratégia na TI, e ferramenta estratégica.

Com relação à variável “níveis de segurança”, constatou-se que hoje não há política de segurança da informação formalizada. A política em discussão, com prazo para entrar em vigor (até final de 2008), abrange os 3 níveis. Assim, os resultados não se encaixam com os apresentados por Oliva (2003), ou seja, de que uma política de segurança da informação deve possuir 3 níveis: diretrizes, normas e procedimentos. No entanto, até final de 2008 este item deverá ter sido atendido, conforme expressa a equipe envolvida no projeto.

Em relação à variável “impacto no negócio”, a instituição de fomento EC3 está sujeita à mesma Lei Complementar nº 105/2001 (Lei do Sigilo Bancário), o que requer um tratamento adequado do cadastro de clientes de instituições financeiras e dos seus dados

financeiros. O impacto de uma quebra de confidencialidade, portanto, é crítico. Da mesma forma que ocorre com os bancos EC1 e EC2, a alteração indevida de informações pode implicar a perda de credibilidade da instituição diante de seus clientes. O único aspecto que não é tão crítico, no caso de EC3, é a disponibilidade, pelo fato de não existirem contas correntes e que, neste caso, as exigências do BACEN não são iguais aos demais casos.

A variável “apoio da diretoria” mostrou que a diretoria da instituição financeira apóia a segurança da informação. Foi nomeado um funcionário para redigir uma Política de Segurança da Informação, com base na ABNT ISO 17799:2005, e definir ações a serem executadas durante o ano de 2008.

Mesmo considerando que as políticas não estejam ainda implantadas, é visível o apoio da diretoria, confirmando o que diz a norma ABNT ISO 17799:2005: “A diretoria deve estabelecer uma clara orientação da política, alinhada com os objetivos do negócio e demonstrar apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização”.

A variável “conformidade” demonstrou que, também no caso de EC3, a conformidade (com leis, regulamentos e contratos) é crítica, especialmente a conformidade com as resoluções do BACEN, como a Resolução 3.380 (“Risco Operacional”). Há providências em andamento, mas não se pode dizer que a segurança da informação, neste momento, contribua neste sentido.

Não foi possível verificar para este caso (pelo menos antes da implantação da política de segurança em 2008) o que é recomendado pela norma ABNT ISO 17799:2005: “A política de segurança da informação objetiva prover uma orientação e apoio da direção para a

segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações pertinentes".

Com relação à variável "efeitos da estratégia na TI", a formulação de uma nova estratégia organizacional não considera aspectos relacionados à TI nem à segurança da informação. Não se verifica a proposta de modelo de alinhamento da TI com a política de segurança da informação de Doherty e Fulford (2005a), segundo a qual, após a equipe de estratégia ter conduzido a análise da situação e formulado uma estratégia, seu impacto na política de segurança da informação deverá ser revisto, e a política de segurança modificada, se for o caso, com vistas a adquirir conformidade com a nova estratégia.

Em relação à variável "ferramenta estratégica", um dos sistemas, o Site institucional/*Internet Banking* (restrito à emissão de boletos de pagamento), claramente suporta a estratégia competitiva da empresa.

Assim, foi possível verificar parcialmente os resultados aqui encontrados com os de Oliva (2003), ou seja, de que as organizações utilizam diversos sistemas informatizados que fornecem as informações necessárias para a definição de cenários e para a tomada de decisão, como ferramentas para a implantação da estratégia competitiva.

5.2.2 Variáveis do Elemento Promotor de Alinhamento – Nível Tático

As varáveis do elemento promotor de alinhamento **nível tático** são as seguintes: sistema de medição, políticas específicas, controles de segurança, ciclo de vida dos sistemas, e projetos de TI como ameaça.

A variável “sistemas de medição” demonstrou que não há avaliação do desempenho da gestão da segurança da informação. O conceito de gestão de segurança da informação é incipiente na instituição, e inexiste uma estrutura formal responsável pelo assunto.

Com relação à variável “políticas específicas” foi possível constatar que, neste ponto, há uma convergência de opiniões dos entrevistados da instituição EC3 com os outros dois casos estudados. Todos os entrevistados internos (exceto um único caso) concordam com a ordem de importância das políticas específicas, conforme apresentado no Quadro 12.

Quadro 12
Principais Políticas de Segurança de Informação

Ordem	Política de Segurança da Informação
1	Conformidade com a legislação e cláusulas contratuais
2	Gestão da continuidade do negócio
3	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa

Existe uma estrutura específica para tomar conta da gestão da continuidade do negócio, exigência da Resolução 3.380 do BACEN, mas os outros dois itens apontados não possuem políticas específicas. Desta forma, é possível dizer que são satisfeitos parcialmente os requisitos da ABNT ISO 17799:2005, a qual recomenda,

> a adoção de políticas específicas, que devem abranger política de segurança organizacional, política de classificação e controle de ativos da informação, política de segurança em pessoas, política de segurança física e do ambiente, política de gerenciamento das operações e comunicações, política de controle de acesso, política de desenvolvimento e manutenção de sistemas, política de gestão de continuidade de negócio e política de continuidade.

A variável “controles de segurança” não se encontra completamente implementada por não existir uma Política de Segurança da Informação institucionalizada e não terem sido explicitados quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas. No entanto, diversos controles e procedimentos já são uma prática corrente ou estão em estágio avançado de implantação.

Desta forma, pode-se considerar que haja atendimento parcial do requisito da ABNT ISO 17799:2005, ou seja, “devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhoria nos existentes”.

Em relação à variável “ciclo de vida dos sistemas”, foi possível constatar que a segurança da informação não faz parte do ciclo de vida dos sistemas, apesar de haver algumas iniciativas neste sentido.

Embora muito tenha sido feito no último ano, não se pode considerar que a segurança participe do ciclo de vida dos sistemas através de validação de processos nas fases pré-desenvolvimentos e de auditorias nas aplicações nas fases de testes. Portanto, esta prática não atende à exigência de que “as organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas” (BERNARDES e MOREIRA, 2005).

Em relação à variável “projetos de TI como ameaça”, foi possível constatar que os projetos de TI não são avaliados para saber de que forma podem se constituir numa ameaça à segurança da informação. Tal atitude não atende a regra expressa por Doherty e Fulford (2005a), de que cada projeto de TI – documentado no PESI – deva ser avaliado criticamente para identificar as possíveis ameaças que representa.

5.2.3 Variáveis do Elemento Promotor de Alinhamento – Nível Operacional

As varáveis do elemento promotor de alinhamento **nível operacional** são as seguintes: consciência da segurança da informação (usuários finais dos sistemas), consciência da segurança da informação (clientes), relacionamento com usuários, documentação, critérios de aceitação e controles.

Em relação à variável “consciência da segurança da informação (usuários finais dos sistemas” foi possível constatar que os usuários finais dos sistemas são treinados informalmente no uso dos mesmos, sem maiores preocupações com o seu uso seguro. Falta um esforço maior no sentido da implantação de uma “consciência da segurança da informação”, levantada por diversos autores, entre eles Kruger e Kearney (2006).

A variável “consciência da segurança da informação (clientes)” demonstrou que o *website* da instituição de fomento EC3 possui um *link* contendo a Política de Segurança; aliás, a disponibilização de informações nos *websites* das instituições financeiras sobre segurança da informação aos usuários é prática comum. Não há, no entanto, nenhuma outra forma de comunicação aos clientes sobre o assunto. Repete-se, novamente, o desconhecimento dos aspectos relacionados à segurança por parte dos clientes, embora a consciência da segurança da informação por parte dos clientes não seja crítica neste caso específico. Não se pode falar que exista a “consciência da segurança da informação”, como apontado por Kruger e Kearney (2006), por parte dos clientes da instituição de fomento EC3.

Em relação à variável “relacionamento com usuários”, constatou-se que, no caso em estudo, existe uma resolução da diretoria que aponta, de forma restrita, direitos e responsabilidades dos usuários. A Política de Segurança da Informação que será implantada abordará o assunto com mais profundidade.

Pode-se dizer que há um atendimento parcial ao que diz a norma ABNT ISO 17799:2005, quando a mesma afirma que a política de segurança da informação deve estabelecer direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização; o relacionamento com os usuários precisa ser claro e bem definido.

Em relação à variável "documentação", foi possível verificar a existência de documentação parcial dos sistemas, por vezes desatualizada, de forma semelhante com o que ocorre nas outras duas instituições financeiras estudadas (EC1 e EC2). Porém, não se verifica o que é preconizado por O'Brien (2001), de que a documentação do projeto dos sistemas e *software* e a operação do sistema deve ser desenvolvida e mantida atualizada.

Quanto à variável "critérios de aceitação", verificou-se que existe um ambiente específico de desenvolvimento de sistemas (o que é uma das boas práticas apontadas pela ABNT ISO 17799:2005). Estão sendo implantados critérios de aceitação para novos sistemas, atualizações e novas versões, com testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação. Em alguns sistemas mais sensíveis a problemas, esta sistemática já está em uso.

Assim, pode-se dizer que a boa prática proposta pela norma ABNT ISO 17799:2005 – "Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e devem ser efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação" – é satisfeita parcialmente.

Em relação à variável "controles", verificou-se que não há sistema formal de medição. Os sistemas do *mainframe*, voltados ao negócio da instituição, funcionam de forma estável, sem maiores problemas de segurança. Os problemas se concentram na plataforma baixa, onde

se constata um crescimento rápido e não planejado da infra-estrutura. No entanto, os controles básicos contra códigos maliciosos existem. Controles e procedimentos carecem de amadurecimento.

Sendo assim, a norma ABNT ISO 17799:2005, que diz que devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários, é atendida parcialmente.

5.2.4 Variáveis do Elemento Promotor de Alinhamento – Infra-estrutura

As varáveis do elemento promotor de alinhamento **infra-estrutura** são as seguintes: diferencial competitivo, confiabilidade, e métricas.

A variável “diferencial competitivo” estabelece se a infra-estrutura representa ou não diferencial competitivo. A avaliação de novas tecnologias de infra-estrutura relativamente plataforma baixa é feita informalmente. Não há existência de um *checklist* contendo todos os aspectos a serem verificados. No caso do mainframe, no qual são executados os sistemas críticos, a avaliação é feita em conjunto por técnicos da instituição e da empresa fornecedora. Não é diferencial competitivo.

Novamente, é fortalecida a afirmação de Davenport (1998) de que, embora o funcionamento correto e adequado desta infra-estrutura seja crítico, a aquisição de tecnologias infra-estruturais raramente significa uma vantagem competitiva em si. O que é vantagem competitiva não é a infra-estrutura propriamente dita, mas sim os projetos que ela suporta.

Em relação à variável “confiabilidade”, verificou-se que a infra-estrutura (plataforma baixa) está, em parte, desatualizada, e requer otimização. Ocorrem problemas de falhas e indisponibilidade. A parte do *mainframe* (sistemas críticos) tem se mostrado bastante confiável (*hardware*), mas não há contingência.

Embora a infra-estrutura não seja diferencial competitivo, o crescimento e o sucesso das organizações, segundo Bernardes e Moreira (2005), atualmente estão diretamente relacionados à necessidade de se manter uma infra-estrutura de TI segura e confiável, o que se verifica parcialmente (em relação aos sistemas críticos).

Em relação à variável “métricas”, verifica-se que não há sistema formal de métricas de segurança da informação da infra-estrutura; novamente, está previsto para 2008. No entanto, a infra-estrutura referente aos sistemas críticos (*mainframe*) está sob controle, sem maiores problemas.

São atendidos parcialmente (em relação ao ambiente dos sistemas críticos) os requisitos da ABNT ISO 17799:2005: “As redes devem ser adequadamente gerenciadas e controladas, de forma a serem protegidas contra ameaças; deve ser mantida a segurança de sistemas que utilizam estas redes, incluindo a informação em trânsito”.

5.2.5 Convergências Gerais entre os elementos do Caso 3 e da literatura

Os principais elementos encontrados resultantes do estudo de caso 3 e aqueles identificados na literatura encontram-se apresentados no Quadro 13. Resumidamente, temos

que o caso mostra atender plenamente 3 variáveis encontradas na literatura, atende parcialmente 8 variáveis e não atende 9 das variáveis.

Quadro 13
Comparação das Dimensões, Elementos e Variáveis do Caso 3 com as Variáveis do Modelo Preliminar

Dimensões	Elementos	Variáveis Preliminares	Atendimento
Negócio	Nível Estratégico	Níveis de segurança	Não atendido (política em implantação irá atender)
		Impacto no negócio	Plenamente atendido
		Apoio da diretoria	Plenamente atendido
TI	Nível Estratégico	Conformidade	Não atendido
		Efeitos da estratégia na TI	Não atendido
		Ferramenta estratégica	Parcialmente atendido (somente *website*)
Negócio	Nível Tático	Sistema de medição	Não atendido
		Políticas específicas	Parcialmente atendido (apenas gestão da continuidade do negócio)
TI	Nível Tático	Controles de segurança	Parcialmente atendido (há alguns controles e procedimentos)
		Ciclo de vida dos sistemas	Não atendido
		Projetos de TI como ameaça	Não atendido
Negócio	Nível Operacional	Consciência da segurança da informação (usuário dos sistemas)	Não atendido
		Consciência da segurança da informação (cliente)	Não atendido
		Relacionamento com usuários	Parcialmente atendido (resolução da diretoria)
TI	Nível Operacional	Documentação	Não atendido (documentações inexistentes ou desatualizadas)
		Critérios de aceitação	Parcialmente atendido
		Controles	Parcialmente atendido (existem controles e procedimentos que carecem de amadurecimento)
Negócio & TI	Infra-Estrutura	Diferencial competitivo	Plenamente atendido (não é diferencial competitivo)
		Confiabilidade	Parcialmente atendido (infra-estrutura dos sistemas críticos é confiável)
		Métricas	Parcialmente atendido (existe gerenciamento e controle da infra-estrutura dos sistemas críticos)

Esta instituição financeira não atende grande parte dos requisitos apontados na literatura. Em parte isto se explica porque não possui contas correntes nem transações *on-line*,

as quais são extremamente vulneráveis e exigem um investimento pesadíssimo em segurança. Mas, os níveis de alinhamento entre segurança e negócio, praticados na instituição de fomento EC3, deveriam ser muito mais significativos. Isto já foi reconhecido pela diretoria, e em 2008 serão desencadeados diversos processos relativos ao assunto.

Na dimensão “Negócio”, elemento “Nível Estratégico”, a variável “níveis de segurança” não é atendida no caso EC3, pois não existe política de segurança da informação formalizada; a política em discussão será implantada em 3 níveis, mas o fato é que atualmente esta variável não é atendida; a variável “impacto no negócio” é plenamente atendida, à medida que qualquer quebra de confidencialidade ou de integridade das informações pode acarretar impactos profundos no negócio; no caso de uma quebra de disponibilidade, o impacto poderá ser pouco importante; a variável “apoio da diretoria” é plenamente atendida, pois a diretoria tem manifestado apoio claro às iniciativas que visam garantir a segurança da informação.

Na dimensão “TI”, elemento “Nível Estratégico”, a variável “conformidade” não é atendida, embora haja providências em andamento neste sentido; a variável “efeitos da estratégia na TI” não é atendida, pois a formulação de uma nova estratégia organizacional não considera aspectos relacionados à TI nem à segurança da informação; a variável “ferramenta estratégica” é parcialmente atendida (somente o *website*), no que este caso se assemelha aos outros dois casos estudados.

Na dimensão “Negócio”, elemento “Nível Tático”, a variável “sistema de medição” não é atendida, pois não há avaliação do desempenho da gestão da segurança da informação. O conceito de gestão de segurança da informação é incipiente na instituição, na qual inexiste uma estrutura formal responsável pelo assunto; a variável “políticas específicas” revelou que

há uma convergência de opiniões dos entrevistados da instituição EC3 com os outros dois casos estudados (exceto um entrevistado no banco EC2), conforma o Quadro 14.

Quadro 14
Principais Políticas de Segurança de Informação

Ordem	Política de Segurança da Informação
1	Conformidade com a legislação e cláusulas contratuais
2	Gestão da continuidade do negócio
3	Requerimentos de treinamento em segurança da informação aos colaboradores da empresa

Na dimensão “TI”, elemento “Nível Tático”, a variável “controles de segurança” é parcialmente atendida, pois existem alguns controles e procedimentos, mas os mesmos não são explicitados em uma política de segurança da informação formalizada; a variável “ciclo de vida dos sistemas” não é atendida, embora haja diversas iniciativas neste sentido; a variável “projetos de TI como ameaça” também não é atendida, pois os novos projetos de TI não são encarados desta maneira.

Na dimensão “Negócio”, elemento “Nível Operacional”, a variável “consciência da segurança da informação (usuário dos sistemas)” não é atendida, porque os usuários finais dos sistemas são treinados informalmente no uso dos mesmos, sem maiores preocupações com a segurança; a variável “consciência da segurança da informação (cliente)” não é atendida, embora haja um *link* contendo a Política de Segurança no *website* da instituição; a variável “relacionamento com usuários” é parcialmente porque, embora não exista (ainda) uma política de segurança da informação formalizada, existe uma resolução da diretoria, de âmbito mais restrito que uma política, mas que legisla sobre o assunto.

Na dimensão “TI”, elemento “Nível Operacional”, a variável “documentação” não é atendida: as documentações são muitas vezes desatualizadas, e por vezes não existem; a variável “critérios de aceitação” é parcialmente atendida, uma vez que existe um ambiente específico de desenvolvimento de sistemas e estão sendo implantados critérios de aceitação para novos sistemas, atualizações e novas versões, com testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação; a variável “controles” é parcialmente atendida, porque muitos controles existem, principalmente no ambiente do *mainframe*, mas os procedimentos carecem de amadurecimento.

No elemento “Infra-estrutura”, a variável “diferencial competitivo” é plenamente atendida, à medida que a infra-estrutura não pode realmente ser considerada como diferencial competitivo; a variável “confiabilidade” é parcialmente atendida, principalmente no ambiente do mainframe, onde são executados os sistemas críticos; a variável “métricas” é parcialmente atendida, pois existem gerenciamento e controle da infra-estrutura dos sistemas críticos.

5.3 COMPARATIVO ENTRE OS ESTUDOS DE CASO

Os Quadros 15, 16, 17 e 18 abaixo mostram uma comparação entre as variáveis de cada nível (elemento do modelo) das dimensões estudadas Negócio e TI do modelo de pesquisa preliminar, convergentes e divergentes entre os casos agrupados (EC1 + EC2) e o caso contraste EC3.

Os padrões comuns (os chamados *frameworks*) de TI encontrados são: padrão de auditoria do BACEN: COBIT; padrão de governança de TI: ITIL; padrão de projetos de TI: CMMI; padrão de segurança da informação: ABNT ISO 17799:2005. No caso da instituição

financeira que não possui contas correntes, estes padrões estão sendo discutidos e já existem projetos de implantação de pelo menos um destes padrões (ABNT ISO 17799:2005), com prazo definido (final de 2008). É interessante ressaltar que não há discrepância entre os *frameworks* utilizados; apenas no caso EC3 a implementação dos mesmos se encontra defasada em relação aos casos EC1 e EC2.

Pode-se reconhecer os *frameworks* acima, especialmente o COBIT, que vem sendo crescentemente utilizado nas auditorias do BACEN, como um fator habilitador de alinhamento estratégico, pois preconiza que as melhores práticas de TI serão cada vez mais alinhadas ao negócio. O ITIL (na versão em uso, a versão 2), foca na TI mas tem a visão do negócio. Também a norma ABNT ISO 17799:2005 (*framework* de segurança) fala em alinhamento entre segurança da informação e negócio. Também será considerado fator habilitador de alinhamento estratégico.

5.3.1 Nível Estratégico

As variáveis consideradas no nível estratégico são: níveis de segurança, impacto no negócio, apoio da diretoria, conformidade, efeitos da estratégia na TI e ferramenta estratégica. As variáveis que forem verificadas no modelo serão consideradas como elementos habilitadores do alinhamento estratégico; aquelas variáveis que não se verificarem serão consideradas como aquelas cuja ausência é elemento inibidor do mesmo alinhamento estratégico.

Quadro 15
Comparação das Dimensões, Elementos e Variáveis em Nível Estratégico convergentes entre os 3 Casos

Dimensões	Elementos	Variáveis Preliminares	Atendimento EC1 + EC2	Atendimento EC3
Negócio	Nível Estratégico	Níveis de segurança	Plenamente atendido	Não atendido (política em implantação irá atender)
		Impacto no negócio	Plenamente atendido	Plenamente atendido
		Apoio da diretoria	Plenamente atendido	Plenamente atendido
TI	Nível Estratégico	Conformidade	Plenamente atendido	Não atendido
		Efeitos da estratégia na TI	Plenamente atendido	Não atendido
		Ferramenta estratégica	Parcialmente atendido (somente *websites*)	Parcialmente atendido (somente *website*)

Em relação à variável “níveis de segurança”, verifica-se que os três níveis (estratégico, tático e operacional), tradicionais nas organizações (O´BRIEN, 2001), são também válidos para a segurança da informação (OLIVA, 2003). Esta correspondência de níveis citada na literatura, que foi tomada como base para o Modelo Preliminar para Estudo, é verificada nos casos estudados (EC1 + EC2), e também é verificada pela iniciativa do caso EC3, com relação à Política de Segurança da Informação que está sendo implantada. Podemos considerar a Política de Segurança da Informação em três níveis como um fator habilitador de alinhamento estratégico, e a sua ausência, como fator inibidor de alinhamento estratégico.

Em relação à variável “impacto no negócio”, sabe-se que o setor bancário é bastante sensível à quebra de confidencialidade das informações, por conta da Lei Complementar nº 105/2001 (Lei do Sigilo Bancário). Quebra de confidencialidade é crime. Portanto, qualquer quebra de confidencialidade das informações é absolutamente crítica. Além das penalidades legais, pode resultar num grande impacto para a imagem pública da empresa. A existência de

contas correntes expõe a informação em mais canais, mas o sigilo tem de ser preservado em todos os casos. A indisponibilidade das informações certamente resultará na perda de negócios, em especial, o *homebanking-officebanking* e o comércio eletrônico, e igualmente em dano severo à imagem. A alteração indevida de informações (quebra de integridade) pode implicar a perda de credibilidade da instituição diante de seus clientes, além de processos judiciais. Qualquer quebra de confidencialidade, integridade ou disponibilidade das informações no setor bancário é absolutamente crítica, salvo a disponibilidade da informação no caso EC 3. O impacto no negócio, em função do que foi apresentado nos casos estudados, inclusive envolvendo aspectos legais, é um fator habilitador de alinhamento estratégico.

Em relação à variável "apoio da diretoria", é sabido que não há dificuldade, nos três casos estudados, quanto ao apoio das respectivas diretorias. Instituições com contas correntes tendem a nomear um diretor específico, profissional, para supervisionar a segurança da informação. A apoio da diretoria é um fator habilitador de alinhamento estratégico.

Dentro deste item, surgiu um aspecto que se mostrou muito relevante, que havia sido levantado por Lessa (2006) e por Von Solms (2006), ao preconizar a presença de estruturas organizacionais que forcem uma boa segurança da informação, e foi confirmado nos estudos de caso EC1 e EC2, diz respeito ao posicionamento hierárquico da Segurança da Informação. Nestes casos, existe uma estrutura específica para Segurança da Informação, hierarquicamente equivalente à TI, sendo Segurança da Informação e TI subordinados à mesma diretoria; estas instituições financeiras não trabalham com subordinação da Segurança da Informação à TI. O estudo de caso EC3, que não atende ou atende apenas parcialmente à maioria dos itens da pesquisa, ainda posiciona a Segurança da Informação como subordinada à TI. Assim, podemos considerar que o posicionamento hierárquico da Segurança da Informação no mesmo nível da TI é fator habilitador de alinhamento estratégico, e o posicionamento

hierárquico da Segurança da Informação subordinada à TI é fator inibidor do alinhamento estratégico.

Em relação à variável "conformidade**",** pode-se dizer que a conformidade (com leis, regulamentos, contratos e estratégias organizacionais) é crítica no setor estudado, que está fazendo um esforço muito grande para alcançar a conformidade com as resoluções do BACEN, especialmente a Resolução 3.380 ("Risco Operacional"). As auditorias do BACEN tendem a ser cada vez mais rígidas, amparadas em legislações e regulamentações específicas, e com base no COBIT. Os casos EC1 e EC2 atendem este requisito; no entanto, no Estudo de Caso 3 percebe-se que a segurança da informação, neste momento, não contribui neste sentido, embora haja providências em andamento. A conformidade constitui-se em fator habilitador de alinhamento estratégico; a falta de conformidade, por outro lado, constatada no caso EC3, é fator inibidor do alinhamento estratégico.

Em relação à variável "efeitos da estratégia na TI", fica claro que, nos três casos estudados, sempre há um risco de que a formulação de uma nova estratégia organizacional afete a TI e a segurança da informação. Nos casos EC1 e EC2 existe a prática de a formulação de novas estratégias levarem em consideração a segurança da informação, ao contrário do que atualmente ocorre com o caso EC3 (embora este assunto faça parte da política de segurança da informação que está sendo implantada). Confirma-se a preocupação (e em dois casos, a prática) com o impacto das novas estratégias na TI e a segurança da informação, conforme alertado por Doherty e Fulford (2005a). Assim, os efeitos da estratégia na TI constituem-se num fator habilitador de alinhamento, e a sua ausência, num fator inibidor.

Em relação à variável "TI como ferramenta estratégica", percebe-se que em todos os casos estudados, embora não se tenha conseguido obter maiores detalhes sobre o uso dos

sistemas internos das instituições, pelo menos os *websites* institucionais/*Internet Banking* (restrito à emissão de boletos de pagamento, no caso EC3), claramente suportam a estratégia competitiva das empresas, o que confirma parcialmente a afirmação de Oliva (2003), de que as organizações utilizam diversos sistemas informatizados para a implantação da estratégia competitiva. Então, pelo menos nos sites institucionais/*Internet Banking* (e certamente nos sistemas de apoio à decisão), a TI é uma ferramenta estratégica, contando como fator habilitador de alinhamento.

5.3.2 Nível Tático

As variáveis consideradas no nível tático são: sistema de medição, políticas específicas, controles de segurança, ciclo de vida dos sistemas e projetos de TI como ameaça.

Em relação à variável "sistema de medição", as instituições financeiras estudadas não praticam uma avaliação formal do desempenho da gestão da segurança da informação (avaliação da adequação das normas de segurança da informação às estratégias empresariais e regulamentações pertinentes). Medidas comentadas na literatura, tais como ROI (*Return on Investment*) e outras, não são praticadas, embora haja uma tentativa de quantificação de retorno em termos de danos evitados, em pelo menos um dos casos estudados. Verifica-se, nos casos EC1 e EC2, o atendimento parcial da avaliação da segurança, embora não haja referência ao uso da norma ABNT ISO 27001 em nenhum dos casos. No caso EC3, não se verifica a existência de um sistema de medição do desempenho da gestão da segurança da informação. Embora a literatura, principalmente a ABNT ISO 17799:2005, aponte para a importância da existência de um eficiente sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria,

não se pode confirmar que um sistema de medição formal seja, de fato, fator habilitador de alinhamento estratégico.

Quadro 16
Comparação das Dimensões, Elementos e Variáveis em Nível Tático convergentes entre os 3 Casos

Dimensões	Elementos	Variáveis Preliminares	Atendimento EC1 + EC2	Atendimento EC3
Negócio	Nível Tático	Sistema de medição	Parcialmente atendido (não há medidas formais)	Não atendido
		Políticas específicas	Plenamente atendido	Parcialmente atendido (apenas gestão da continuidade do negócio)
TI	Nível Tático	Controles de segurança	Parcialmente atendido (há dúvidas sobre a divulgação dos controles)	Parcialmente atendido (há alguns controles e procedimentos)
		Ciclo de vida dos sistemas	Plenamente atendido	Não atendido
		Projetos de TI como ameaça	Parcialmente atendido (processo carece de amadurecimento)	Não atendido

Em relação à variável "políticas específicas**"**, nota-se que todas as instituições financeiras estudadas concordam com a ordem de importância das políticas específicas. A mais importante é a conformidade com a legislação e cláusulas contratuais; em segundo lugar vem a gestão da continuidade do negócio, seguida pelos requerimentos de treinamento em segurança da informação aos colaboradores da empresa. Nos casos EC1 e EC2, estas políticas específicas existem, validando o requisito da ABNT ISO 17799:2005, a qual "recomenda a adoção de políticas específicas, que devem abranger política de segurança organizacional, política de classificação e controle de ativos da informação, política de segurança em pessoas,

política de segurança física e do ambiente, política de gerenciamento das operações e comunicações, política de controle de acesso, política de desenvolvimento e manutenção de sistemas, política de gestão de continuidade de negócio e política de continuidade". No caso EC3, existe uma estrutura específica para tomar conta da gestão da continuidade do negócio validando, portanto, parcialmente o requisito da norma. Claramente, a existência de políticas específicas é fator habilitador de alinhamento estratégico.

Em relação à variável "controles de segurança**",** as instituições financeiras EC1 e EC2 explicitam os controles e procedimentos de segurança que devem ser incorporados aos sistemas; no entanto, parece haver desconhecimento destas regras por parte do pessoal de TI, em um dos casos. Já o caso EC3, apesar de não contar com uma Política de Segurança da Informação institucionalizada, utiliza ou está implementando diversos controles e procedimentos. Assim, pode-se considerar que, em todos os casos, haja atendimento parcial do requisito da ABNT ISO 17799:2005, quando esta diz que "devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhoria nos existentes". A existência de controles de segurança é fator habilitador de alinhamento estratégico, pois todas as instituições bancárias estudadas estão investindo muito esforço no assunto.

Em relação à variável "ciclo de vida dos sistemas", nos casos EC1 e EC2, a segurança da informação participa do ciclo de vida dos sistemas através de validação de processos nas fases pré-desenvolvimentos e de auditorias nas aplicações nas fases de testes, validando plenamente a exigência de Bernardes e Moreira (2005), de que "as organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas". No caso EC3, não se pode considerar que a segurança participe do ciclo de vida dos sistemas, pois não há validação de processos nas fases pré-desenvolvimentos nem auditorias nas aplicações nas

fases de testes. A participação da segurança da informação no ciclo de vida dos sistemas é fator habilitador de alinhamento estratégico, e a sua ausência é fator inibidor do alinhamento.

Em relação à variável "projetos de TI como ameaça", verificou-se que os casos EC1 e EC2 fazem a avaliação de que forma cada sistema pode se constituir num risco à segurança da informação. Porém, em ambos os casos este processo parece não estar suficientemente amadurecido. O caso EC3 ainda não avalia seus projetos com este objetivo. Assim, poder-se dizer que, no primeiro caso (EC1 + EC2), é atendido parcialmente o que dizem Doherty e Fulford (2005a), de que cada projeto de TI – documentado no PESI – deva ser avaliado criticamente para identificar as possíveis ameaças que representa; no segundo caso (EC3), não é atendido. A avaliação de que forma cada sistema pode se constituir numa ameaça à segurança da informação pode ser considerado fator habilitador de alinhamento estratégico, e a sua falta como fator inibidor.

5.3.3 Nível Operacional

As variáveis consideradas no nível operacional são: consciência da segurança da informação (usuários finais dos sistemas), consciência da segurança da informação (clientes), relacionamento com usuários, documentação, critérios de aceitação e controles.

Em relação à variável "consciência da segurança da informação (usuários finais dos sistemas)", percebe-se que, nos casos EC1 e EC2, percebe-se um esforço considerável no sentido de treinar adequadamente os usuários finais sobre segurança da informação e no uso seguro dos sistemas. Pode-se considerar que existe uma "consciência da segurança da informação", levantada por diversos autores, entre eles Kruger e Kearney (2006). O mesmo

não ocorre no caso EC3. Podemos, então, considerar a consciência da segurança da informação (usuários finais dos sistemas) como fator habilitador de alinhamento estratégico, e a sua ausência como fator inibidor de alinhamento.

Quadro 17
Comparação das Dimensões, Elementos e Variáveis em Nível Operacional convergentes entre os 3 Casos

Dimensões	Elementos	Variáveis Preliminares	Atendimento EC1 + EC2	Atendimento EC3
Negócio	Nível Operacional	Consciência da segurança da informação (usuário dos	Plenamente atendido	Não atendido
		Consciência da segurança da informação (cliente)	Parcialmente atendido (não há *feedback* sobre consciência do cliente)	Não atendido
		Relacionamento com usuários	Plenamente atendido	Parcialmente atendido (resolução da diretoria)
TI	Nível Operacional	Documentação	Não atendido (documentações inexistentes ou desatualizadas)	Não atendido (documentações inexistentes ou desatualizadas)
		Critérios de aceitação	Plenamente atendido	Parcialmente atendido
		Controles	Parcialmente atendido (existem controles; procedimentos carecem de amadurecimento)	Parcialmente atendido (existem controles e procedimentos que carecem de amadurecimento)

Em relação à variável "consciência da segurança da informação (clientes)", percebe-se um esforço muito importante nos casos EC1 e EC2. Não há, no entanto, nenhum *feed-back* em relação a como o cliente se sente em relação à segurança. Apesar do grande esforço realizado, não há elementos para se afirmar que exista, entre os clientes, uma "consciência da segurança da informação", como apontado por Kruger e Kearney (2006), o que somente se verifica parcialmente. Já no caso EC3, esta conscientização do cliente não se verifica.

Consideramos a falta de consciência da segurança da informação (clientes) como fator inibidor do alinhamento estratégico.

Em relação à variável "relacionamento com usuários", nos casos EC1 e EC2, as respectivas políticas de segurança da informação estabelecem direitos e responsabilidades, inclusive limites a terceirizados e estagiários. Existem instrumentos como termo de compromisso para o uso de sistemas, informações e recursos de TI da empresa. É seguida a norma ABNT ISO 17799:2005, quando a mesma afirma que a política de segurança da informação deve estabelecer direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização; o relacionamento com os usuários precisa ser claro e bem definido. No caso EC3, inexiste uma política de segurança da informação institucionalizada, mas há uma resolução da diretoria que estabelece regras para o uso de alguns recursos de TI, verificando o cumprimento parcial deste item da norma. As políticas de relacionamento com usuários (estabelecimento de direitos e responsabilidades, inclusive limites a terceirizados e estagiários, cartilhas, termos de compromisso) constituem fator habilitador de alinhamento estratégico.

Em relação à variável "documentação", a documentação dos projetos e da operação dos sistemas existe, mas nem sempre está atualizada, em todos os casos estudados. Há sistemas em que a documentação é completa e atualizada, há sistemas em que ela simplesmente não existe. No entanto, de uma forma genérica, pode-se afirmar que não é atendido o preconizado por O'Brien (2001), de que as documentações do projeto dos sistemas e *software* e da operação dos sistemas devem ser desenvolvidas e mantidas atualizadas. Pelo fato de nenhum dos casos estudados de fato preencher este requisito, e de não se perceber um esforço muito grande das instituições financeiras estudadas neste sentido, não podemos

considerar a documentação dos projetos e sistemas como sendo fator habilitador de alinhamento estratégico.

Em relação à variável “critérios de aceitação”, nos casos EC1 e EC2, existe um ambiente específico de desenvolvimento de sistemas (uma das boas práticas apontadas pela ABNT ISO 17799:2005). Existe uma metodologia de gerenciamento de mudanças, baseada em melhores práticas de gestão de infra-estrutura (ITIL). É satisfeita a boa prática proposta pela norma ABNT ISO 17799:2005: “Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e devem ser efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação”. No caso EC3, este processo está sendo implementado (ainda sem o ITIL), mas carece de amadurecimento, o que leva a um atendimento parcial deste item da norma. Consideramos o ambiente e procedimentos que favoreçam o estabelecimento de critérios de aceitação de sistemas e projetos de TI como um fator habilitador do alinhamento estratégico.

Em relação à variável “controles”, no caso das três instituições financeiras estudadas, existem controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança, mas a questão dos procedimentos parece não estar bem resolvida. Há procedimentos de monitoramento isolados, que não abrangem ainda todos os sistemas. É parcial o atendimento à norma ABNT ISO 17799:2005, quando ela diz que devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários. Há um grande esforço, por parte das instituições estudadas, para a melhoria dos seus controles. Consideramos os controles como fator habilitador de alinhamento estratégico.

5.3.4 Infra-estrutura

As variáveis consideradas no nível da Infra-estrutura (Quadro 18) são: diferencial competitivo, confiabilidade, e métricas.

Em relação à variável “diferencial competitivo”, embora varie, nas três instituições financeiras estudadas, a forma como a infra-estrutura é avaliada e homologada, não há referências a ser um diferencial competitivo. O que é vantagem competitiva não é a infra-estrutura propriamente dita, mas sim os projetos que ela suporta; desta forma, é validada a afirmação de Davenport (1998) de que, embora o funcionamento correto e adequado desta infra-estrutura seja crítico, a aquisição de tecnologias infra-estruturais raramente significa uma vantagem competitiva em si. No entanto, o fato de a infra-estrutura não ser um diferencial competitivo não pode ser considerado fator habilitador de alinhamento estratégico.

Em relação à variável “confiabilidade”, percebe-se que nos casos das EC1 e EC2, a confiabilidade, segurança e estabilidade da infra-estrutura são consideradas ponto forte, pois qualquer tipo de instabilidade pode comprometer seriamente a segurança da informação. O mesmo ocorre em relação à infra-estrutura dos sistemas críticos (em *mainframe*) do caso EC3, embora não ocorra em relação à infra-estrutura da plataforma baixa, que comporta sistemas menos críticos. Atende-se, nestes casos, o preconizado por Bernardes e Moreira (2005), ou seja, o crescimento e o sucesso das organizações atualmente estão diretamente relacionados à necessidade de se manter uma infra-estrutura de TI segura e confiável. A confiabilidade, bem como a segurança e a estabilidade da infra-estrutura de TI, pode ser considerada fator habilitador de alinhamento estratégico.

Quadro 18
Comparação das Dimensões, Elementos e Variáveis de Infra-estrutura convergentes entre os 3 Casos

Dimensões	Elementos	Variáveis Preliminares	Atendimento EC1 + EC2	Atendimento EC3
Negócio & TI	Infra-Estrutura	Diferencial competitivo	Plenamente atendido (não é diferencial competitivo)	Plenamente atendido (não é diferencial competitivo)
		Confiabilidade	Plenamente atendido	Parcialmente atendido (infra-estrutura dos sistemas críticos é confiável)
		Métricas	Plenamente atendido	Parcialmente atendido (existe gerenciamento e controle da infra-estrutura dos sistemas críticos)

Em relação à variável “métricas”, no que diz respeito a gerenciamento e controle da rede, os casos EC1 e EC2 atendem os requisitos da ABNT ISO 17799:2005: “As redes devem ser adequadamente gerenciadas e controladas, de forma a serem protegidas contra ameaças; deve ser mantida a segurança de sistemas que utilizam estas redes, incluindo a informação em trânsito”. O mesmo ocorre em relação à infra-estrutura dos sistemas críticos (em mainframe) do caso EC3, embora não ocorra em relação à infra-estrutura da plataforma baixa, que comporta sistemas menos críticos. Apesar da importância das métricas de controle da infra-estrutura, dificilmente poderíamos considerá-las como sendo fator habilitador de alinhamento estratégico.

5.4 CONTRAPOSIÇÃO DOS RESULTADOS COM O MODELO PRELIMINAR PARA ESTUDO

No intuito de determinar se as principais características de promoção do alinhamento estratégico entre as políticas e estratégias de segurança de informação a as práticas efetivas da TI elencadas no Modelo Preliminar para Estudo (Figura 2), os resultados apresentados nas seções anteriores foram contrapostos. A descrição encontra-se desmembrada para efeitos de uma análise mais detalhada.

O alinhamento estratégico da dimensão **TI**, mostrado na Figura 5, é garantido por diversos fatores, abrangendo os 3 (três) níveis:

- A necessidade de alinhamento entre TI e negócio imposta pelas auditorias do BACEN, ao utilizar o padrão COBIT;

- A utilização do padrão ITIL, que possui foco na TI, mas é voltado para o negócio (OGC, 2007; BERNARDES e MOREIRA, 2005; ITGI, 2005);

- A necessidade de conformidade com leis, regulamentos, contratos e estratégias organizacionais (ABNT, 2005);

- Os efeitos da estratégia (ou de novas estratégias) sobre a TI e segurança da informação (DOHERTY E FULFORD, 2005a);

- As ferramentas de TI como ferramentas estratégicas - no mínimo, os *websites* (OLIVA, 2003).

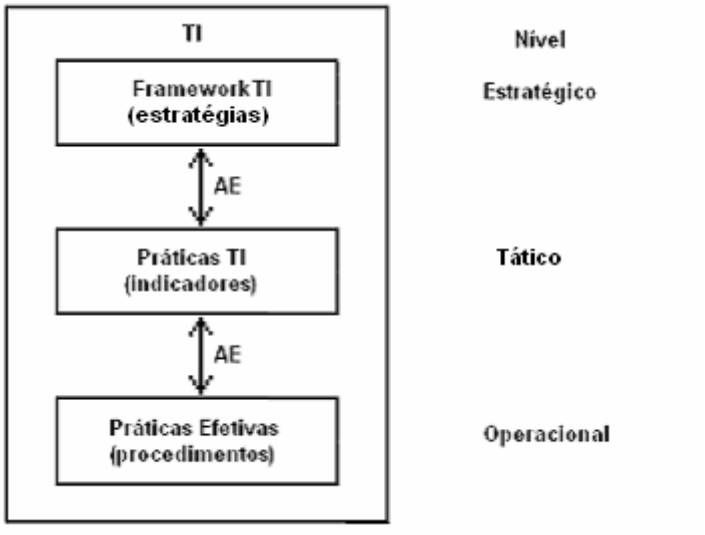

Figura 5 – Modelo Preliminar para Estudo – Alinhamento estratégico da dimensão TI

O alinhamento estratégico da dimensão **Negócio**, mostrado na Figura 6, é garantido pelos fatores abaixo, abrangendo os 3 (três) níveis:

- Emprego da norma ABNT ISO 17799:2005 como *framework* de segurança da informação (OGC, 2007; BERNARDES e MOREIRA, 2005; ITGI, 2005);

- Posicionamento hierárquico da Segurança da Informação no mesmo nível da TI, jamais subordinada à TI (LESSA, 2003);

- Níveis de segurança: a Política de Segurança da Informação em 3 (três) níveis, onde normas de nível tático implementam as diretrizes da diretoria, e os procedimentos operacionais implementam as normas de nível tático (OLIVA, 2003).

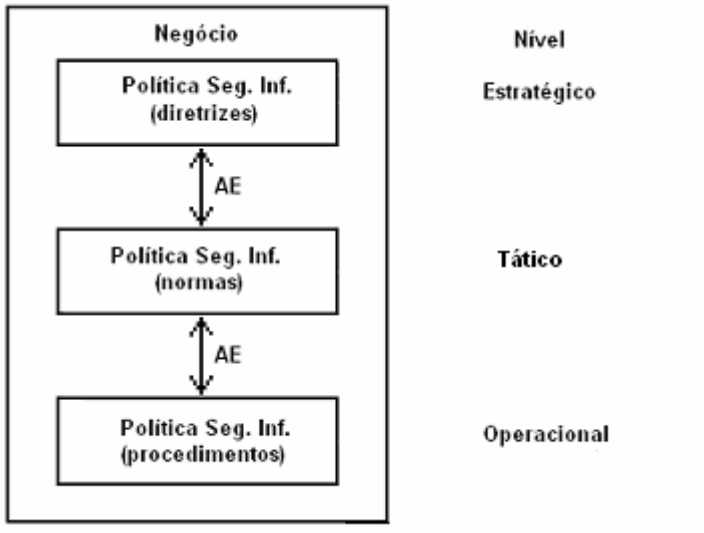

Figura 6 – Modelo Preliminar para Estudo – Alinhamento estratégico da dimensão Negócio

O alinhamento estratégico entre **TI** e **Negócio** (Segurança da Informação) no **nível estratégico**, mostrado na Figura 7, é garantido pelos fatores abaixo:

- Emprego da norma ABNT ISO 17799:2005 como padrão de segurança da informação (OGC, 2007; BERNARDES e MOREIRA, 2005; ITGI, 2005);

- Impacto de quebras de confidencialidade, integridade ou disponibilidade de ativos de TI no negócio (ABNT, 2005);

- Apoio da diretoria, no sentido de promover ações relativas à segurança da informação, basicamente com foco nos ativos de TI (ABNT, 2005);

- A necessidade de conformidade com leis, regulamentos, contratos e estratégias organizacionais (ABNT, 2005).

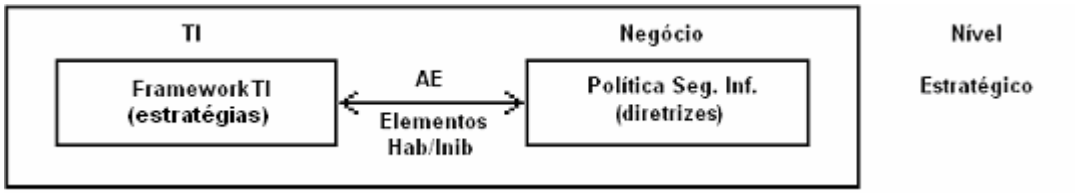

Figura 7 – Modelo Preliminar para Estudo – Nível Estratégico

O alinhamento estratégico entre **TI** e **Negócio** (Segurança da Informação) no **nível tático**, mostrado na Figura 8, é garantido pelos fatores abaixo:

- Existência de políticas específicas, como conformidade com a legislação e cláusulas contratuais; gestão da continuidade do negócio, requerimentos de treinamento dos usuários dos ativos de TI (ABNT, 2005; VON SOLMS, 2006);

- Existência de controles e procedimentos de segurança que devem ser incorporados aos sistemas de TI (ABNT, 2005);

- Participação da segurança da informação no ciclo de vida dos sistemas, através de validação e auditoria de processos em diversas fases do desenvolvimento e teste de sistemas de TI (BERNARDES E MOREIRA, 2005);

- Avaliação de que forma cada sistema pode se constituir num risco à segurança da informação (LANDWEHR, 2001; DOHERTY E FULFORD, 2005a).

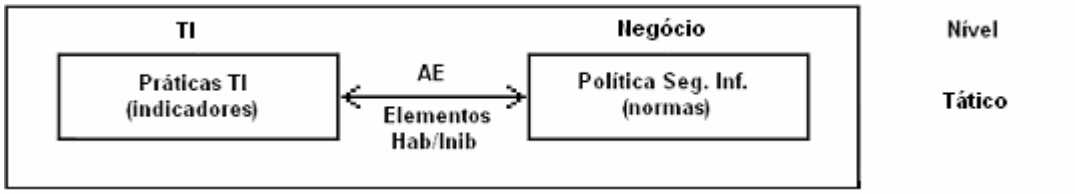

Figura 8 – Modelo Preliminar para Estudo – Nível Tático

O alinhamento estratégico **TI** e **Negócio** (Segurança da Informação) no **nível operacional**, mostrado na Figura 9, é garantido pelos fatores abaixo:

- A consciência da segurança da informação, ou consciência do uso seguro dos recursos de TI, por parte dos usuários internos (ABNT, 2005; KRUGER E KEARNEY, 2006);

- Relacionamento com usuários, ou a existência de políticas de segurança da informação que estabelecem direitos e responsabilidades, inclusive limites a terceirizados e estagiários; instrumentos como termo de compromisso para o uso de sistemas, informações e recursos de TI (ABNT, 2005);

- Existência de ambiente e procedimentos que favoreçam o estabelecimento de critérios de aceitação de sistemas e projetos de TI (ABNT, 2005);

- Existência de controles e procedimentos de detecção, prevenção e recuperação para proteger contra incidentes de segurança em ativos de TI (ABNT, 2005).

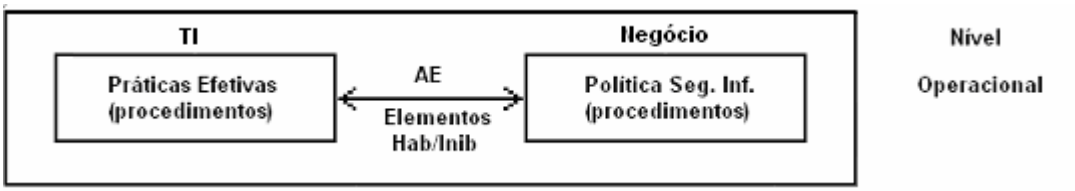

Figura 9 – Modelo Preliminar para Estudo – Nível Operacional

O alinhamento estratégico **TI** e **Negócio** (Segurança da Informação) no nível de **infra-estrutura** é garantido por:

- Confiabilidade, segurança e estabilidade da infra-estrutura que suporta as aplicações de TI (DAVENPORT, 1998; BERNARDES E MOREIRA, 2005).

A partir do exposto, podem-se verificar os elementos e as relações propostas no Modelo Preliminar para Estudo (Figura 2), tanto na dimensão **T**I quanto na dimensão **Negócio**, assim como se pode considerar a existência dos elementos em níveis **estratégico**, **tático** e **operacional**, bem como a infra-estrutura subjacente como promotores do alinhamento entre as políticas e estratégias de segurança de informação e as práticas efetivas de TI.

5.5 FATORES HABILITADORES E INIBIDORES

Esta seção mostra a convergência dos principais fatores habilitadores e inibidores da promoção do alinhamento estratégico entre as políticas e estratégias de segurança de informação e as práticas efetivas de TI. Nem todas as variáveis preliminares inicialmente propostas (Quadro 2) foram possíveis de serem verificadas porém, outras foram acrescentadas. A partir dos resultados apurados, foi possível elaborar um novo quadro de

dimensões, elementos e variáveis, relacionando ainda os fatores habilitadores e inibidores de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI (Quadro 19).

Quadro 19
Fatores Habilitadores e Inibidores da Promoção do Alinhamento Estratégico entre as Políticas de Segurança de Informação e as Estratégias e Práticas de TI

Dimensões/ Elementos	Variáveis preliminares	Variáveis confirmadas	Fator Habilitador	Fator Inibidor
Negócio Nível Estratégico	Níveis de segurança	Níveis de segurança	Sim	Sim
	Impacto no negócio	Impacto no negócio	Sim	-
	Apoio da diretoria	Apoio da diretoria	Sim	-
	-	Posicionamento hierárquico da Seg. Informação	Sim	Sim
	-	*Framework* Segurança (ABNT ISO 17799)	Sim	-
TI Nível Estratégico	Conformidade	Conformidade	Sim	Sim
	Efeitos da estratégia na TI	Efeitos da estratégia na TI	Sim	Sim
	Ferramenta estratégica	Ferramenta estratégica	Sim	-
	-	*Frameworks* TI (COBIT, ITIL)	Sim	-
Negócio Nível Tático	Sistema de medição	-	-	-
	Políticas específicas	Políticas específicas	Sim	-
TI Nível Tático	Controles de segurança	Controles de segurança	Sim	-
	Ciclo de vida dos sistemas	Ciclo de vida dos sistemas	Sim	Sim
	Projetos de TI como ameaça	Projetos de TI como ameaça	Sim	Sim
Negócio Nível Operacional	Consciência da segurança da informação (usuário dos sistemas)	Consciência da segurança da informação (usuário dos sistemas)	Sim	Sim
	Consciência da segurança da informação (cliente)	Consciência da segurança da informação (cliente)	-	Sim
	Relacionamento com usuários	Relacionamento com usuários	Sim	-

TI Nível Operacional	Documentação	-	-	-
	Critérios de aceitação	Critérios de aceitação	Sim	-
	Controles	Controles	Sim	-
Infra-Estrutura	Diferencial competitivo	-	-	-
	Confiabilidade	Confiabilidade	Sim	-
	Métricas	-	-	-

As variáveis relativas à dimensão **TI**, elemento **nível estratégico**, são:

- A variável "conformidade", sugerida pela literatura (ABNT, 2005; VON SOLMS, 2006), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, e a sua ausência, como fator inibidor;

- A variável "efeitos da estratégia na TI", sugerida na literatura (DOHERTY E FULFORD, 2005a), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico, e a sua ausência, como fator inibidor;

- A variável "ferramenta estratégica", sugerida na literatura (OLIVA, 2003), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico (pelo menos os *websites* analisados);

- A variável "*frameworks* de TI (ITIL) e de auditoria (COBIT), que não fazia parte das "Dimensões, elementos e variáveis preliminares de pesquisa" (Quadro 2), foi incluída a partir da pesquisa e de referências na literatura

(BERNARDES e MOREIRA, 2005) como fator habilitador de alinhamento estratégico.

As variáveis relativas à dimensão **Negócio**, elemento **nível tático**, são:

- A variável "sistema de medição", sugerida pela literatura (ABNT, 2005; ABNT, 2006), não foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, pois em nenhum dos casos estudados ela está de fato implementada;

- A variável "políticas específicas", sugerida pela literatura (ABNT, 2005; VON SOLMS, 2006), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico.

As variáveis relativas à dimensão **TI**, elemento **nível tático**, são:

- A variável "controles de segurança", sugerida pela literatura (ABNT, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI;

- A variável "ciclo de vida dos sistemas", sugerida na literatura (BERNARDES E MOREIRA, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico, e a sua ausência, como fator inibidor;

- A variável "projetos de TI como ameaça", sugerida na literatura (LANDWEHR, 2001; DOHERTY E FULFORD, 2005a), foi confirmada na

pesquisa como fator habilitador de alinhamento estratégico, e a sua ausência, como fator inibidor.

As variáveis relativas à dimensão **Negócio**, elemento **nível operacional**, são:

- A variável "consciência da segurança da informação (usuário dos sistemas)", sugerida na literatura (ABNT, 2005; KRUGER E KEARNEY, 2006), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, e a sua ausência, como fator inibidor;

- A variável "consciência da segurança da informação (clientes)", sugerida na literatura (ABNT, 2005; KRUGER E KEARNEY, 2006), não foi confirmada na pesquisa como fator habilitador de alinhamento estratégico, em virtude de nenhum dos casos estudados possuírem um conhecimento real de como o cliente se comporta diante da problemática, mas a sua ausência foi confirmada como fator inibidor;

- A variável "relacionamento com usuários", sugerida na literatura (ABNT, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico.

As variáveis relativas à dimensão **TI**, elemento **nível operacional**, são:

- A variável "documentação", sugerida na literatura (O'BRIEN, 2001), não foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas

adotadas na TI, pelo motivo de que nenhuma das instituições financeiras pesquisadas possui, de fato, a documentação relativa aos sistemas totalmente atualizada;

- A variável "critérios de aceitação", sugerida na literatura (ABNT, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico;

- A variável "controles", sugerida na literatura (ABNT, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico.

As variáveis relativas às dimensões **Negócio & TI**, elemento **infra-estrutura**, são:

- A variável "diferencial competitivo", sugerida na literatura (DAVENPORT, 1998), não foi confirmada na pesquisa como fator habilitador de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, porque não há como justificar que o fato de a infra-estrutura não ser um diferencial competitivo possa, de fato, ser considerado fator habilitador de alinhamento estratégico;

- A variável "confiabilidade", sugerida na literatura (DAVENPORT, 1998; BERNARDES E MOREIRA, 2005), foi confirmada na pesquisa como fator habilitador de alinhamento estratégico;

- A variável "métricas", sugerida na literatura (SWANSON ET AL., 2003; ABNT, 2005), não foi confirmada na pesquisa como fator habilitador de alinhamento estratégico, porque nenhum dos casos estudados possui de fato controle absoluto sobre todas as métricas de que fala a literatura.

6 CONCLUSÕES

O objetivo principal desta pesquisa, de identificar as principais características da promoção do alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI para os níveis estratégico, tático e operacional, bem como os fatores habilitadores e inibidores deste alinhamento foi atendido, uma vez que foi possível determinar as relações de alinhamento entre as dimensões negócio e TI e os principais elementos de promoção deste alinhamento entre os níveis estratégico, tático, operacional e de infra-estrutura. Vale destacar que fica constatada a afirmação da maioria dos autores de que a infra-estrutura de TI para suporte a segurança da informação em instituições financeiras não significa maior vantagem competitiva (VON SOLMS, 2006; OLIVA, 2003; STRAUB e WELK, 1998; HENDERSON e VENKATRAMAN, 1993).

No caso das instituições financeiras brasileiras não há diferenciações regionais no que diz respeito a regulamentações ou normas governamentais a serem seguidas. As normas são as mesmas, e é o mesmo órgão (o BACEN) que audita as instituições financeiras, com base nos mesmos padrões (atualmente convergindo para o COBIT). O estudo restringiu-se a instituições financeiras com atuação no Rio Grande do Sul apenas por conveniência, não por questões referentes a eventuais mecanismos regulatórios diferenciados, ou eventuais respostas diferenciadas às regulamentações.

Embora haja uma diferença muito grande entre os estudos de caso referentes às instituições financeiras que possuem contas correntes (EC1 e EC2), se as compararmos à instituição financeira de fomento, que não possui contas correntes (EC3), não se pode afirmar cabalmente que a existência de contas correntes seja fator suficiente para determinar esta diferença, pois a citada instituição financeira de fomento está implantando uma política de

segurança da informação, com base na ABNT ISO 17799:2005, da mesma forma que as outras instituições financeiras estudadas. Parece, pois, tratar-se mais de um processo pouco maduro de alinhamento entre as práticas de segurança e as políticas do negócio. Vale destacar que o foco desta dissertação não foi verificar a maturidade das práticas, mas apenas verificar a sua existência.

Assim, mantendo o agrupamento dos estudos de caso referentes às instituições financeiras que possuem contas correntes, por um lado, e o estudo de caso referente à instituição financeira que não possui contas correntes, pelo outro lado, percebe-se uma tendência clara de apostar no alinhamento estratégico da segurança da informação, no setor bancário brasileiro. É certo que a existência de contas correntes, com todos os canais de acesso (internet *banking*, terminais de atendimento automático, acesso via celular, cartões de crédito e de débito, etc.) exige uma resposta mais rápida e eficaz da segurança da informação, com foco no negócio, mas a sua ausência não impede nem desaconselha este mesmo alinhamento.

As principais políticas, normas e resoluções de segurança de informação e principais estratégias e práticas de segurança da informação dos departamentos de TI dos casos estudados, de uma forma geral, são:

- Criação de uma estrutura específica para a Segurança da Informação, com o mesmo nível hierárquico da TI (exceto em um dos casos estudados);

- Uso da norma ABNT ISO 17799:2005, com todas (ou quase todas) as suas boas práticas, entre elas: políticas específicas, política de senhas, controles de segurança, conscientização dos usuários de sistemas sobre segurança da informação, normas para relacionamento com usuários, estabelecimento de

critérios de aceitação de sistemas, segregação de ambientes de desenvolvimento e produção, segregação de funções de desenvolvimento e teste/homologação, controles e procedimentos de segurança, etc.;

- Política de Segurança da Informação em 3 níveis implantada ou em implantação;

- Política de Classificação da Informação implantada ou em implantação;

- Política de Continuidade de Negócios implantada ou em implantação.

A partir da aplicação do instrumento de pesquisa (Apêndice C), foi possível a obtenção de resultados que, contrapostos com o Modelo Preliminar para Estudo (Figura 2), mostram as evidências da existência dos elementos promotores de alinhamento entre as políticas e estratégias de segurança de informação do negócio e as efetivas práticas adotadas pela TI. Os resultados mostraram algumas alterações na composição das variáveis (Quadro 19) com relação às variáveis iniciais de pesquisa (Quadro 2).

Da mesma forma, os resultados dos estudos de caso permitiram relacionar alguns dos principais **fatores habilitadores** de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI, listados a seguir:

1. **Apoio ativo da Diretoria** (LESSA, 2006; PELTIER, 2002), com claro direcionamento e demonstrando comprometimento; prioridade para projetos que envolvem segurança da informação; patrocínio do sistema de gestão de segurança da informação;

2. **Criação de estrutura específica de Segurança da Informação** (LESSA, 2006), posicionada hierarquicamente no mesmo nível que a TI (jamais subordinada à TI); atualmente se percebe uma tendência de migração da área de Segurança da Informação da Diretoria de TI para a Diretoria de Segurança ou de Riscos. Pode-se incluir neste item a observação de Lessa (2006) a respeito da importância da liderança do projeto [de segurança da informação] por um executivo que não pertença à área de TI;

3. **Política de Segurança da Informação configurada em 3 (três) níveis** (HENDERSON e VENKATRAMAN, 1993) estratégico (resoluções da diretoria contendo diretrizes), tático (normas gerais criadas a partir das diretrizes) e operacional (normas específicas e manuais);

4. A ameaça do **impacto de uma quebra de confidencialidade, integridade ou disponibilidade** da informação no negócio (OLIVA, 2003), que pode ser extremamente severo. Diante da Lei Complementar nº 105/2001 (“Lei do Sigilo Bancário”) uma quebra de confidencialidade da informação, que pode facilmente redundar numa violação do sigilo de informações, pode se constituir em crime – portanto, seu impacto é sempre alto;

5. **Conformidade com leis, regulamentações específicas**, padrões relevantes (no caso bancário, a conformidade com a Resolução 3.380 do BACEN é crítica), contratos e diretrizes estratégicas corporativas (VON SOLMS, 2006);

6. **Aderência a padrões de TI**, como COBIT e ITIL, e segurança da informação, como a norma ABNT ISO 17799:2005;

7. **Os efeitos da estratégia (ou de novas estratégias) sobre a TI e segurança da informação**, pois novas estratégias podem, eventualmente, criar novas vulnerabilidades (DOHERTY e FULFORD, 2005ª);

8. As **ferramentas de TI** como ferramentas estratégicas (no mínimo, os *websites*) (OLIVA, 2003);

9. **Existência de políticas específicas** (VON SOLMS, 2006), como conformidade com a legislação e cláusulas contratuais, gestão da continuidade do negócio (também exigido pela Resolução 3.380 do BACEN), requerimentos de treinamento dos usuários dos ativos de TI;

10. **Controles e procedimentos de segurança incorporados aos sistemas** (ABNT, 2005;2006): a Política de Segurança da Informação deve explicitar estes controles e procedimentos;

11. **Participação da segurança da informação no ciclo de vida dos sistemas (**BERNARDES e MOREIRA, 2005) através da validação dos processos nas fases de pré-desenvolvimento e da auditoria das aplicações nas fases de testes; a metodologia de desenvolvimento de sistemas deve incluir normas de segurança;

12. **Projetos de TI** como ameaça (DOHERTY e FULFORD, 2005a; LANDWEHR, 2001): deve ser feita a avaliação de que forma cada sistema pode se constituir num risco à segurança da informação;

13. A **consciência da segurança da informação** (KRUGER e KEARNEY, 2006), ou a consciência do uso seguro dos recursos de TI, por parte dos usuários internos;

14. **Relacionamento com usuários** (ABNT, 2005): as políticas de segurança da informação devem estabelecer direitos e responsabilidades, inclusive limites a terceirizados e estagiários; devem existir instrumentos como termo de compromisso para o uso de sistemas, informações e recursos de TI da empresa;

15. **Critérios de aceitação de sistemas** (ABNT, 2005), com segregação de ambientes de desenvolvimento e produção, segregação de funções de desenvolvimento e teste/homologação;

16. **Controles e procedimentos** de prevenção, detecção e recuperação contra incidentes de segurança (ABNT, 2005);

17. **Confiabilidade, segurança e estabilidade da infra-estrutura** que suporta as aplicações de TI (BERNARDES e MOREIRA, 2005; DAVENPORT, 1998).

A partir dos resultados desta pesquisa também foi possível obter alguns dos principais **fatores inibidores** de alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI encontrados, listados a seguir:

1. **Pouca importância para a Segurança da Informação**, com seu posicionamento hierárquico subordinado à TI;

2. **Ausência de Política de Segurança da Informação formalizada**, constituídas nos 3 níveis (estratégico, tático e operacional) (O'BRIEN, 2001);

3. **Falta de conformidade com leis, regulamentações específicas**, padrões relevantes e estratégias corporativas (VON SOLMS, 2006);

4. **Efeitos negativos não detectados de novas estratégias corporativas na TI e na segurança da informação** (DOHERTY e FULFORD, 2005a);

5. **A segurança da informação não fazendo parte do ciclo de vida dos sistemas** (BERNARDES e MOREIRA, 2005);

6. Ameaças não detectadas de **projetos de TI** à segurança da informação (LANDWEHR, 2001);

7. **Falta de consciência do uso seguro dos sistemas por parte dos usuários internos** (KRUGER e KEARNEY, 2006);

8. **Falta de consciência do uso seguro dos sistemas por parte dos clientes** (KRUGER e KEARNEY, 2006): fragilidade do usuário (especialmente do *homebanking*): dificuldade de disseminação da política de segurança, ingenuidade no uso de ferramentas bancárias na Internet/ terminais eletrônicos, suscetibilidade à engenharia social.

6.1 LIMITAÇÕES DA PESQUISA

As limitações desta pesquisa se devem, principalmente, à relativamente restrita disponibilidade de informações, uma vez que as políticas de segurança de duas das instituições financeiras estudadas não permitiram maior aprofundamento, nem tampouco análise de documentos em alguns casos, bem como a pouca disposição de pessoas não vinculadas à segurança da informação para responder sobre este assunto.

Diante disto, julgou-se interessante listar algumas das principais limitações encontradas: (a) pesquisa realizada no setor financeiro, o que permite certa generalização, mas que a princípio é válida apenas para este setor; (b) seleção de instituições financeiras com atuação no Rio Grande do Sul, por conveniência; (c) realização de entrevistas principalmente com pessoas vinculadas à segurança da informação e TI, pois as pessoas mais vinculadas às áreas de negócio não se consideraram aptas a responder as questões; e, (d) não ter sido possível uma investigação com mais profundidade da relação entre segurança da informação e governança de TI.

6.2 CONTRIBUIÇÕES DA PESQUISA

As principais contribuições desta pesquisa tanto de cunho acadêmico quanto prático são as seguintes: (a) confirmação do uso da norma ABNT ISO 17799:2005 como padrão para a implantação de política de segurança nas instituições bancárias com atuação no Rio Grande do Sul; como as normatizações e regulamentações do setor são de nível nacional e não estadual, o mesmo ocorrendo com a citada norma, pode-se inferir que esta afirmação tenha uma abrangência nacional, e não apenas regional; (b) o assunto em foco nesta dissertação carecia de maiores estudos; por um lado, havia ampla literatura sobre alinhamento estratégico, com enfoque acadêmico e pesquisas realizadas em organizações; por outro lado, havia uma relativamente grande quantidade de artigos sobre segurança da informação, de caráter prático, pouco acadêmico. A presente dissertação vem somar-se a alguns poucos trabalhos acadêmicos, tais como Oliva (2003) e Lessa (2006), no sentido de refletir sobre o alinhamento estratégico da segurança da informação; e, (c) no caso específico da instituição financeira de fomento, na qual foi realizado o Estudo de Caso 3, os subsídios representados por este trabalho serão utilizados para a implantação da sua Política de Segurança da Informação.

6.3 PESQUISAS FUTURAS

Em função da amplitude e da relevância do tema, sugere-se como pesquisas futuras que possam dar continuidade a esta, os seguintes tópicos: (a) conscientização do cliente (correntista) por parte das instituições financeiras: o que de fato é feito para aumentar a segurança da informação pelo lado do cliente, quais os procedimentos recomendados, que tipo de *software* de segurança são utilizados, como é avaliada a conscientização do cliente, de que forma se poderia de fato atingir o cliente para conscientizá-lo; (b) consciência da segurança da informação por parte do cliente (correntista): este item poderia ser explorado com mais profundidade, certamente por meio de uma *survey*, que questionasse quais os procedimentos que o cliente adota, de que forma ele é conscientizado; e, (c) estrutura de segurança da informação: onde se encaixa nas instituições financeiras a segurança da informação, qual seu nível hierárquico, a que diretoria está subordinada, quais as suas funções (age como órgão normatizador, consultor, ou executor, ou auditor).

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma NBR ISO/IEC 17799**: **Tecnologia da Informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2001.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma NBR ISO/IEC 17799**: **Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma NBR ISO/IEC 27001**: **Sistema de Gestão de Segurança da Informação (SGSI)**. Rio de Janeiro, 2006.

ALBERTIN, A. L. **Pesquisa FGV-EAESP de comércio eletrônico no mercado brasileiro: resumo**. 6.ed. São Paulo: FGV/EAESP/CIA, 2005. Disponível em: <http://www.fgvsp.br/academico/estudos/cia/ned.htm>. Acesso em: 01 de agosto de 2006.

BACEN 2004. **Sistema de Informações de Crédito do Banco Central**. Disponível em: http://www.bcb.gov.br/fis/crc/ftp/cartilhascr.pdf. Acesso em: 29 de outubro de 2007.

BAGUETE. 2006. **V Debaguete – Observatório Crítico da TI Sul**. Disponível em <http://www.debaguete.com.br/05/index.php>. Acesso em 05 de outubro de 2007.

BAGUETE, 2007. **Guilherme Lessa - Segurança não tem fim, só começo**. Disponível em < http://www.baguete.com.br/entrevista.php?id=195>. Acesso em 24 de setembro de 2007.

BALBO, L.O. **Uma Abordagem Correlacional dos Modelos CobiT / ITIL e da Norma ISO 17799 para o tema Segurança da Informação**. 2007. In: Escola Politécnica da Universidade de São Paulo, Departamento de Engenharia de Computação e Sistemas Digitais. 56 fl.

BANRISUL. **Política de Segurança**. 2007. Disponível em <http://www.bcb.gov.br/fis/crc/ftp/cartilhascr.pdf>. Acesso em: 24 de setembro de 2007.

BENBASAT, I.; GOLDSTEIN, D. K.; MEAD, M. **The Case Research Strategy in Studies of Information Systems**. MIS Quarterly, pp. 369-386, Sep., 1987.

BERNARDES, M. C.; MOREIRA, E. S. **Um modelo para inclusão da Governança da Segurança da Informação no escopo da Governança Organizacional**. 2005. SSI 2005 - 7th Intl Symposium on System and Information Security. Disponível em <http://www.linorg.cirp.usp.br/SSI/SSI2005/artigos/14275.pdf>. Acesso em: 20 de janeiro de 2007.

BRITO, O. S. **Gestão de riscos: uma abordagem orientada a riscos operacionais**. São Paulo, Ed. Saraiva, 2007.

BRODBECK, A. F. **Alinhamento estratégico entre os Planos de Negócio e de Tecnologia de Informação**: um modelo operacional para implementação. Tese de Doutorado do Programa de Pós-Graduação em Administração. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2001.

BRODBECK, A. F.; HOPPEN, N. **Modelo de Alinhamento para Implementação dos Planos de Negócio e de Tecnologia de Informação**. In: Encontro Anual da ANPAD, 24, 2000, Santa Catarina. Anais eletrônicos ... Santa Catarina: ANPAD, 2000.

BRODBECK, A. F.; HOPPEN, N.; RIGONI, E. H.; CANEPA, P. C. V. **Práticas de Alinhamento Estratégico Promovidas em Organizações do Estado do Rio Grande do Sul. Brasília,** ENANPAD 2003.

CARNEIRO, F.L.; VIVAN, G.F.A.; KRAUSE, K. **O novo Acordo da Basiléia – Um estudo de caso para o contexto brasileiro**. 2005. Disponível em <http://www4.bcb.gov.br/pre/inscricaoContaB/trabalhos/O%20Novo%20Acordo%20de%20Basil%C3%A9ia_um%20estudo%20de%20caso%20para%20o%20contexto%20brasileiro.pdf>. Acesso em 04 de setembro de 2007.

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. 2007. Disponível em <http://www.cert.br/stats/incidentes/>. Acesso em 30 de janeiro de 2007.

CIAB – Revista CIAB FEBRABAN nº 07 – Outubro 2006. Disponível em <http://www.ciab.org.br/portugues/Revistas/07Outubro06.pdf>. Acesso em 05 de setembro de 2007.

CIBORRA, C. **De profundis ? Deconstructing the concept of strategic alignment**. In: IRIS CONFERENCE, 20., 1997, Norway. Proceedings… Norway : University of Oslo, 1997.

COMPUTERWORLD. 2006. Disponível em <http://computerworld.uol.com.br/seguranca/2006/06/21/idgnoticia.2006-06-21.1766126313>. Acesso em 05 de setembro de 2007.

CSI/FBI. **CSI/FBI COMPUTER CRIME AND SECURITY SURVEY**. 2006. Computer Security Institute.

DAVENPORT, T. H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação**. 1998. Editora Futura, São Paulo.

DOHERTY, N. F.; FULFORD, H. **Aligning the information security policy with the strategic information systems plan.** Computers & Security 2005;25:55-63.

DOHERTY, N. F.; FULFORD, H. **Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analisys.** Information Resources Management Journal; Oct-Dec 2005; 18, 4; ABI/INFORM Global, pg. 21.

EZINGEARD, J. McCFADZEAN, E. e BIRCHALL D. **A Model of Information Assurance Benefits**. Information Systems Management, Spring 2005, p.20-29

FISMA. **Federal Information Security Management Act (FISMA) 2004 Report to Congress**, 2004. Disponível em: <http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf>. Acesso em 07 de julho de 2006.

FRANKFORT-NACHMIAS, C.; NACHMIAS, D. **Research methods in the social sciences**. 5. Ed. New York: St. Martin's Press, 1996.

FREITAS, H. e JANISSEK, R. **Análise Léxica e Análise de Conteúdo: técnicas complementares, seqüências e recorrentes para análise de dados qualitativos**. Porto Alegre: Sphinx-Sagra (distrib.). 2000, 176p.

GODOI, C. K.; MATTOS, P. L. C. L. de. Entrevista qualitativa: instrumento de pesquisa e evento dialógico. In: GODOI, C. K.; MELO, R. B.; BARBOSA, A. **Pesquisa Qualitativa em Estudos Organizacionais - Paradigmas, Estratégias e Métodos**. São Paulo: Saraiva, 2006. p. 301-323.

GONÇALVES, L. R. O. **O surgimento da Norma Nacional de Segurança de Informação [NBR ISO/IEC-1779:2001]**. 2004. Disponível em: < E:\PPGA\Textos\Segurança\Lockabit\O surgimento da Norma Nacional de Segurança de Informação NBR ISO IEC-1779 2001].htm>. Acesso em: 23 de outubro de 2007.

HENDERSON, J. C.; VENKATRAMAN, N. **Strategic alignment: leveraging information technology for transforming organizations**. IBM Systems Journal, v. 32, n. 1, p. 4-16, 1993.

HOPPEN, N. **Avaliação de artigos de pesquisa em sistemas de informação: proposta de um guia**. XXI ENCONTRO NACIONAL DA ASSOCIAÇÃO NACIONAL DOS PROGRAMAS DE POSGRADUAÇAO EM ADMINISTRAÇÃO, 1997, Anais ... Rio de Janeiro: ENAPAD, 1997 CD-ROM.

IPIB – Internet Produto Interno Bruto. 2007. Disponível em: <http://www.ipib.com.br/gloss.asp?origem=mapasite>. Acesso em: 27 de março de 2007.

ITGI - IT Governance Institute. **Aligning COBIT, ITIL and ISO 17799 for Business Benefit**. 2005. Disponível em: <http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490>. Acesso em: 17 de julho de 2006

ITGI - IT Governance Institute. **COBIT**. 2006. Disponível em: <http://www.isaca.org/cobit>. Acesso em: 17 de julho de 2006.

ITIL - IT SERVICE MANAGEMENT ZONE. 2007. Disponível em: <http://www.itil.org.uk/>. Acesso em: 13 de maio de 2007.

KRUGER, H. A.; KEARNEY, W. D. **A prototype for assessing information security awareness.** Computers & Security 25(2006);289–296.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais: Administrando a Empresa Digital**. 5a Edição. 2004. Pearson - Prentice-Hall.

LANDWEHR, C.E. **Computer Security**. International Journal of Information Security, 2001, 1(1), 3-13.

LEDERER, A. L.; SETHI, V. **The Implementation of Strategic Information System Planning Methodologies**. MIS Quarterly, p. 445-461, Sep. 1988.

LESSA, G. G. **Gestão da Segurança da Informação: Implementação da Norma BS 17799-2:2—2 em uma Instituição Financeira.** Dissertação de Mestrado do Programa de Pós-Graduação em Administração. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2006. 108 f

LUFTMAN, J. N.; **Assessing business-IT alignment maturity**. Communications of the Association for Information Systems, v.4 Article 14, December, 2000.

LUFTMAN, J. N.; LEWIS, P.R.; OLDACH, S.H. **Transforming the enterprise: the alignment of business and information technology strategies**. IBM System Journal**,** Armonk, v. 32, n.1, p. 198-220, 1993.

LUFTMAN, J. N.; PAPP, R.; BRIER, T. **Enablers and Inhibitors of Business-IT alignment**. Communications of the Association for Information Systems, v.1 Article 11, March, 1999.

MARTINS, A. B.; SANTOS, C. A. S. **UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO**. 2005. In: Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 2, No. 2, 2005, pp. 121-136.

MAÇADA, A. C. G. ; PICADA, Rodrigo Cassol ; SANTOS, André Moraes dos ; RIOS, Leonardo Ramos. **Governança de Tecnologia de Informação baseado na Metodologia COBIT: O caso de um banco privado brasileiro**. In: XXVI Encontro Nacional de Engenharia de Produção, 2006, Fortaleza. Ética e Responsabilidade Social - a contribuição do engenheiro de produção, 2006. v. 1. p. 1-8.

MODULO. Zilta Penna Marinho. Atribuições do Security Officer. 2005. Disponível em <http://www.modulo.com.br/empresa/site/modulo_interna_cursos_security.jsp?pLinkMenu=Cursos&pMenuPai=3#>. Acesso em 01 de novembro de 2007.

MYERS, M. **Qualitative Research in Information Systems**. 1997. Disponível em <http://www.misq.org/discovery/MISQD_isworld/index.html>. Acesso em 29 de dezembro de 2006.

NAKAMURA, E. T.; GEUS, P. L. Segurança de redes em ambientes corporativos. São Paulo: Berkeley Brasil, 2002.

NIST - National Institute of Standards and Technology; **An Introduction to Computer Security: The Nist HandBook**. 1996. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-12/>. Acesso em 13 de março de 2006.

O'BRIEN, J. A. **Sistemas de Informação e as decisões gerenciais na era da internet**. São Paulo. Saraiva, 2001.

OGC - The United Kingdom's Office of Government Commerce. 2007. Disponível em <http://www.itil.co.uk/>. Acesso em 29 de dezembro de 2006.

OLIVA, R. P. **A importância da política de segurança da informação de acordo com a NBR/ISO 17799 na estratégia competitiva.** Dissertação de Mestrado em Administração. Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre, 2003. 158 f.

PELTIER, T. R. **Why Security Fails**. Peltier Associates. Disponível em: <www.securetangent.com/download/whySecurityFails2002.pdf>. Acesso em 04 de julho de 2006.

PEREIRA, C. M. L. **Fatores Promotores e Inibidores do Alinhamento Estratégico da Tecnologia da Informação em uma situação de fusão: o caso de uma rede varejista**. Dissertação de Mestrado do Programa de Pós-Graduação em Administração. Universidade Federal de Pernambuco. Recife, 2006. 166 f.

PEROTTONI, R.; OLIVEIRA,M. LUCIANO, E. M.; FREITAS, H. **Sistemas de informações: um estudo comparativo das características tradicionais às atuais**. ReAd, Porto Alegre, v.7, n.3, 2001.

REICH, B. H.; BENBASAT, I. **Measuring the linkage between business and information technology objectives.** MIS Quarterly, p. 55-81, Mar. 1996.

SÊMOLA, M. **A importância da Gestão da Segurança da Informação**. 2003. Disponível em <http://www.linorg.cirp.usp.br/SSI/SSI2003/Palest/P03-Apresentacao.pdf>. Acesso em 30 de janeiro de 2007.

SIPONEN, Mikko**. Information Security Standards Focus on the Existence of Process Not Its Content.** Communications of the ACM, August 2006/Vol. 49, No. 8;97:100

STRAUB Jr., D. W., & WELKE, R. J. (1998). **Coping with systems risk: Security planning models for management decision making**. MIS Quarterly, 22(4), 441–469.

SWANSON, M.; BARTOL, N.;. SABATO, J.; GRAFFO, L. **Security Metrics Guide for**

Information Technology Systems. Washington, National Institute of Standards and Technology, U.S. Department of Commerce, 2003.

THILOLLENT, Michel. **Metodologia da pesquisa-ação.** São Paulo: Cortez Ed., 1985.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987.

VON SOLMS, Basie. **Information Security – The Fourth Wave**. Computers & Security 2006;25:165-168.

YIN, R. **Estudo de Casos. Planejamento e Métodos**. Ed. Bookman, Porto Alegre, 2005.

APÊNDICE A – REGULAMENTAÇÕES GOVERNAMENTAIS

A partir de situações como a deterioração dos índices de capital dos bancos internacionais na década de 80 e escândalos financeiros ocorridos em empresas como a Enron, Worldcom e outras, já no início do século XXI, as regulamentações legais com atuação em setores específicos da economia têm se tornado cada vez mais intensas. Na área financeira, em nível internacional, pode-se citar o Comitê da Basiléia (composto por autoridades bancárias de diversos países), cujo primeiro "Acordo de Capital da Basiléia", marco regulatório decisivo mundial, data de 1988. Por sua vez, a lei americana Sarbanes-Oxley, de 2002, foi um marco definitivo na gestão de riscos financeiros. A Sarbanes-Oxley (ou apenas SOX) tornou Diretores Executivos e Diretores Financeiros pessoalmente responsáveis por definir, avaliar e monitorar a eficácia dos controles internos sobre relatórios financeiros e divulgações.

Também no Brasil as regulamentações governamentais têm aumentado. Pode-se citar, por exemplo, as resoluções do Banco Central, tais como a 2.554 (Controles Internos) e 3.380 (Risco Operacional), ambas na área financeira, elaboradas a partir do "Acordo da Basiléia", ou o padrão TISS – Troca de Informações em Saúde Suplementar, na área da saúde. Há também regulamentações na área de seguros, cooperativismo, e assim por diante.

Definição de Instituição Financeira

O termo “Instituição Financeira” é definido pela Lei nº 7.492, de 16 de junho de 1986, que define os crimes contra o sistema financeiro nacional, e dá outras providências. Diz o artigo primeiro:

> Art. 1º Considera-se instituição financeira [...] a pessoa jurídica de direito público ou privado, que tenha como atividade principal ou acessória, cumulativamente ou não, a captação, intermediação ou aplicação de recursos financeiros (Vetado) de terceiros, em moeda nacional ou estrangeira, ou a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários.
>
> Parágrafo único. Equipara-se à instituição financeira:
>
> I - a pessoa jurídica que capte ou administre seguros, câmbio, consórcio, capitalização ou qualquer tipo de poupança, ou recursos de terceiros;
>
> II - a pessoa natural que exerça quaisquer das atividades referidas neste artigo, ainda que de forma eventual.

Conforme o Banco Central do Brasil,

> “As instituições financeiras são agentes que, mediante autorização do Banco Central, captam recursos do público, principalmente sob a forma de depósitos. Também concedem empréstimos sob várias modalidades, além de aplicar em outros ativos, tais como títulos do tesouro nacional.”

São instituições financeiras: Bancos Múltiplos, Bancos Comerciais; Caixa Econômica Federal; Bancos de Investimento; Bancos de Desenvolvimento; Sociedades de Crédito Imobiliário; Sociedades de Crédito, Financiamento e Investimento; Companhias Hipotecárias; Agências de Fomento ou de Desenvolvimento; Associações de Poupança e Empréstimo; Sociedades de Arrendamento Mercantil; e Cooperativas de Crédito (BACEN, 2004).

Sintetizando, Brito (2007) diz que instituições financeiras

> "são instituições que atuam no processo de intermediação financeira, compreendendo, sobretudo, diversas modalidades de captação de recursos, operações de crédito, seguros, capitalização, mercado de capitais, poupança e financiamento à habitação, arrendamento mercantil, comércio exterior; sendo essas operações de curto e longo prazos".

Marco Regulatório da Área Financeira

Especificamente na área financeira brasileira, alvo deste trabalho, o BACEN (Banco Central do Brasil) é o principal órgão regulamentador e fiscalizador; também a CVM (Comissão de Valores Mobiliários) tem emitido instruções relevantes. A regulamentação da área financeira é federal, válida igualmente para todas as unidades da federação. Observa-se, no caso brasileiro, uma convergência rumo aos princípios do chamado "Novo Acordo da Basiléia", pois "*evidenciam, em uma primeira análise, que o objetivo geral do Novo Acordo tende a ser alcançado na realidade brasileira*" (CARNEIRO ET AL., 2005).

Os "Acordos da Basiléia"

O objetivo do chamado "Comitê da Basiléia" ("*The Basel Committee*") é a elaboração de padrões de supervisão no setor bancário, bem como recomendações e princípios para as melhores práticas no mercado financeiro. Não possui autoridade formal de supervisão internacional nem suas conclusões têm valor legal. Espera-se que as autoridades (normalmente os bancos centrais) de cada país adotem as medidas necessárias para implementar as suas recomendações. O Comitê da Basiléia foi constituído em 1974, com o patrocínio do BIS ("*Bank for International Settlements*"), sendo composto por representantes dos bancos centrais e autoridades de supervisão bancária da Bélgica, Canadá, França, Alemanha, Itália, Japão, Luxembugo, Holanda, Espanha, Suíça, Suécia, Inglaterra e Estados

Unidos. Em 1988 foi aprovado o primeiro “Acordo de Capital da Basiléia”; recomendava padrões mínimos de requerimento de capital para fazer frente à notória deterioração dos índices de capital dos bancos internacionais na década de 80. O foco principal deste acordo foi o risco de crédito. A aceitação deste acordo foi melhor do que se esperava, tendo sido encarado como um marco na reorientação das estratégias de regulação financeira no final do século XX (CARNEIRO ET AL., 2005).

O documento “Convergência Internacional de Mensuração e Padrões de Capital: Uma Estrutura Revisada”, conhecido como “Novo Acordo de Capital” ou ainda como “Basiléia II”, teve sua versão final publicada em 26 de junho de 2004. Este “Acordo da Basiléia II” propõe o uso de uma nova estrutura para requerimento de capital, baseada em três pilares: o primeiro trata dos requerimentos de capitais com base nos riscos de mercado e de crédito; o segundo reforça a capacidade dos supervisores bancários para avaliar e adaptar os requerimentos de capital às condições individuais das instituições financeiras; e o terceiro atribui à transparência e à divulgação de informações um papel importante e relevante no fomento à disciplina de mercado (CARNEIRO ET AL., 2005).

Iniciativas legais que afetam a segurança da informação

As principais leis, citadas por Brito (2007), que norteiam o ambiente do mercado financeiro, são:

- Lei n. 4131, de 3/9/1962 - Lei do Capital Estrangeiro;

- Lei n. 4.595, de 31/12/1964 - Lei do Sistema Financeiro Nacional;

- Lei n. 4.728, de 14/7/1965 - Lei dos Mercados de Capitais;
- Lei n. 6.024, de 13/3/1974 - Lei de Intervenções e Liquidações;
- Lei n. 7.357, de 2/9/1985 - Lei do Cheque;
- Lei n. 7.492, de 16/6/1986 - Lei do Colarinho Branco/Crimes Financeiros;
- Lei n. 9.069, de 29/6/1995 - Lei do Real;
- Lei n. 9.447, de 14/3/1997 - Lei da Responsabilidade Solidária;
- Lei n. 9613, de 3/3/1998 - Lei da "Lavagem" de Dinheiro;
- Lei n. 10.214, de 27/3/2001 - Lei do Sistema de Pagamentos Brasileiro.

Também deve ser considerada a Lei Complementar nº 105/2001 - Lei do Sigilo Bancário.

O Brasil tem demonstrado uma tendência de aderência aos padrões dos "Acordos da Basiléia". O foco principal tende a ser a gestão de riscos, e a informação passa a exercer papel absolutamente crítico nesse contexto. Dentre as principais iniciativas regulatórias que afetam a segurança da informação no Brasil, especificamente na área financeira, podem ser observados:

- A Resolução 2.554/1998 do Banco Central, de 24 de setembro de 1998, que dispõe sobre a implantação e implementação de controles internos;

- A Instrução CVM n° 358, de 3 de janeiro de 2002, da Comissão de Valores Mobiliários, que dispõe, entre outros tópicos, sobre a divulgação e uso de informações sobre ato ou fato relevante;

- O Decreto n° 4.553, de 27 de dezembro de 2002, da Presidência da República, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

- A Resolução nº 3.380, de 29/06/2006, que dispõe sobre a implementação de estrutura de Gerenciamento do Risco Operacional. Entre os eventos de risco operacional, incluem-se fraudes internas e externas, demandas trabalhistas e segurança deficiente do local de trabalho, práticas inadequadas relativas a clientes, produtos e serviços, danos a ativos físicos próprios ou em uso pela instituição, eventos que acarretem a interrupção das atividades da instituição, falhas em sistemas de tecnologia da informação, falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição. Esta resolução vai no rumo de atender o “Acordo Basiléia II”. A Resolução 3.380 (Apêndice B) não é um conjunto de boas práticas, mas exige que as instituições financeiras implementem a governança de TI. Pelo menos um dos requisitos (“falhas em sistemas de tecnologia da informação”) exige diretamente a implementação de uma política de segurança da informação.

APÊNDICE B – Resolução BACEN 3.380

Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional.

O BANCO CENTRAL DO BRASIL, na forma do art. 9º da Lei 4.595, de 31 de dezembro de 1964, torna público que o CONSELHO MONETÁRIO NACIONAL, em sessão realizada em 29 de junho de 2006, com base nos arts. 4º, inciso VIII, da referida lei, 2º, inciso VI, 8º e 9º da Lei 4.728, de 14 de julho de 1965, e 20 da Lei 4.864, de 29 de novembro de 1965, na Lei 6.099, de 12 de setembro de 1974, com as alterações introduzidas pela Lei 7.132, de 26 de outubro de 1983, na Lei 10.194, de 14 de fevereiro de 2001, com as alterações introduzidas pela Lei 11.110, de 25 de abril de 2005, e no art. 6o do Decreto-lei 759, de 12 de agosto de 1969,

R E S O L V E U:

Art. 1º Determinar às instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil a implementação de estrutura de gerenciamento do risco operacional.

Parágrafo único. A estrutura de que trata o caput deve ser compatível com a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas da instituição.

Art. 2º Para os efeitos desta resolução, define-se como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

§ 1º A definição de que trata o caput inclui o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

§ 2º Entre os eventos de risco operacional, incluem-se:

I - fraudes internas

II - fraudes externas

III - demandas trabalhistas e segurança deficiente do local de trabalho;

IV - práticas inadequadas relativas a clientes, produtos e serviços;

V - danos a ativos físicos próprios ou em uso pela instituição;

VI - aqueles que acarretem a interrupção das atividades da instituição;

VII - falhas em sistemas de tecnologia da informação;

VIII - falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

Art. 3º A estrutura de gerenciamento do risco operacional deve prever:

I - identificação, avaliação, monitoramento, controle e mitigação do risco operacional;

II - documentação e armazenamento de informações referentes às perdas associadas ao risco operacional;

III - elaboração, com periodicidade mínima anual, de relatórios que permitam a identificação e correção tempestiva das deficiências de controle e de gerenciamento do risco operacional;

IV - realização, com periodicidade mínima anual, de testes de avaliação dos sistemas de controle de riscos operacionais implementados;

V - elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados;

VI - existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional;

VII - implementação, manutenção e divulgação de processo estruturado de comunicação e informação.

§ 1º A política de gerenciamento do risco operacional deve ser aprovada e revisada, no mínimo anualmente, pela diretoria das instituições de que trata o art. 1º e pelo conselho de administração, se houver.

§ 2º Os relatórios mencionados no inciso III devem ser submetidos à diretoria das instituições de que trata o art. 1º e ao conselho de administração, se houver, que devem manifestar-se expressamente acerca das ações a serem implementadas para correção tempestiva das deficiências apontadas.

§ 3º Eventuais deficiências devem compor os relatórios de avaliação da qualidade e adequação do sistema de controles internos, inclusive sistemas de processamento eletrônico de dados e de gerenciamento de riscos e de descumprimento de dispositivos legais e regulamentares, que tenham, ou possam vir a ter impactos relevantes nas demonstrações contábeis ou nas operações da entidade auditada,

elaborados pela auditoria independente, conforme disposto na regulamentação vigente.

Art. 4o A descrição da estrutura de gerenciamento do risco operacional deve ser evidenciada em relatório de acesso público, com periodicidade mínima anual.

§ 1º O conselho de administração ou, na sua inexistência, a diretoria da instituição deve fazer constar do relatório descrito no caput sua responsabilidade pelas informações divulgadas.

§ 2º As instituições mencionadas no art. 1º devem publicar, em conjunto com as demonstrações contábeis semestrais, resumo da descrição de sua estrutura de gerenciamento do risco operacional, indicando a localização do relatório citado no caput.

Art. 5º A estrutura de gerenciamento do risco operacional deve estar capacitada a identificar, avaliar, monitorar, controlar e mitigar os riscos associados a cada instituição individualmente, ao conglomerado financeiro, conforme o Plano Contábil das Instituições do Sistema Financeiro Nacional - Cosif, bem como a identificar e acompanhar os riscos associados às demais empresas integrantes do consolidado econômico-financeiro, definido na Resolução 2.723, de 31 de maio de 2000.

Parágrafo único. A estrutura, prevista no caput, deve também estar capacitada a identificar e monitorar o risco operacional decorrente de serviços terceirizados relevantes para o funcionamento regular da instituição, prevendo os respectivos planos de contingências, conforme art. 3º, inciso VI.

Art. 6º A atividade de gerenciamento do risco operacional deve ser executada por unidade específica nas instituições mencionadas no art. 1º.

Parágrafo único. A unidade a que se refere o caput deve ser segregada da unidade executora da atividade de auditoria interna, de que trata o art. 2º da Resolução 2.554, de 24 de setembro de 1998, com a redação dada pela Resolução 3.056, de 19 de dezembro de 2002.

Art. 7º Com relação à estrutura de gerenciamento de risco, admite-se a constituição de uma única unidade responsável:

I - pelo gerenciamento de risco operacional do conglomerado financeiro e das respectivas instituições integrantes;

II - pela atividade de identificação e acompanhamento do risco operacional das empresas não financeiras integrantes do consolidado econômico-financeiro.

Art. 8º As instituições mencionadas no art. 1º devem indicar diretor responsável pelo gerenciamento do risco operacional.

Parágrafo único. Para fins da responsabilidade de que trata o caput, admite-se que o diretor indicado desempenhe outras funções na instituição, exceto a relativa à administração de recursos de terceiros.

Art. 9º A estrutura de gerenciamento do risco operacional deverá ser implementada até 31 de dezembro de 2007, com a observância do seguinte cronograma:

I - até 31 de dezembro de 2006: indicação do diretor responsável e definição da estrutura organizacional que tornará efetiva sua implementação;

II - até 30 de junho de 2007: definição da política institucional, dos processos, dos procedimentos e dos sistemas necessários à sua efetiva implementação;

III - até 31de dezembro de 2007: efetiva implementação da estrutura de gerenciamento de risco operacional, incluindo os itens previstos no art. 3º, incisos III a VII.

Parágrafo único. As definições mencionadas nos incisos I e II deverão ser aprovadas pela diretoria das instituições de que trata o art. 1º e pelo conselho de administração, se houver, dentro dos prazos estipulados.

Art. 10. O Banco Central do Brasil poderá:

I - determinar a adoção de controles adicionais, nos casos de inadequação ou insuficiência dos controles do risco operacional implementados pelas instituições mencionadas no art. 1º;

II - imputar limites operacionais mais restritivos à instituição que deixar de observar, no prazo estabelecido, a determinação de que trata o inciso I.

Art. 11. Esta resolução entra em vigor na data de sua publicação.

Brasília, 29 de junho de 2006.

Henrique de Campos Meirelles
Presidente

APÊNDICE C - Instrumento de Pesquisa

Variável do Modelo	Pergunta
Nível Estratégico	
Segurança da Informação e Negócio	
Níveis de segurança	Quais os níveis de segurança da informação que a empresa possui? (OLIVA, 2003)
Impacto no negócio	Qual o impacto que um problema de segurança da informação pode causar na estratégia competitiva da empresa? Considere: 1. Quebra de confidencialidade das informações 2. Alteração das informações 3. Indisponibilidade das informações (OLIVA, 2003)
Apoio da diretoria	Quais têm sido as ações da diretoria no sentido de apoio e comprometimento com a segurança da informação? (ABNT, 2005)
Segurança da Informação e TI	
Conformidade	Como a segurança da informação contribui para garantir conformidade com padrões relevantes, regulamentações governamentais e contratos? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Efeitos da estratégia na TI	De que forma a formulação de uma nova estratégia organizacional afeta a TI? Como ocorre o processo de definição das respostas da TI às estratégias da empresa? Você considera este fator um ponto forte ou fraco? (DOHERTY e FULFORD, 2005a)
Ferramenta estratégica	Quais os principais sistemas de informação da sua empresa? Como cada um deles dá suporte à estratégia competitiva da empresa? Considere: ( ) Sistema de Gestão (ERP) ( ) Sistema de Relacionamento (CRM) ( ) Sistema de Informação Executiva (EIS) ( ) Supply Chain ( ) Site institucional/Internet Banking ( ) Outros (especificar): _____ Quais os pontos fortes e fracos? (OLIVA, 2003)

Nível Tático	
Segurança da Informação e Negócio	
Sistema de medição	De que forma a empresa avalia o desempenho da gestão da segurança da informação? Você considera este fator um ponto forte ou fraco? (ABNT, 2006)
Políticas específicas	Quais os 3 itens de maior importância na composição da política de segurança da informação? Classifique (1 para o mais importante, 2 para o segundo e 3 para o terceiro): ( ) Conformidade com a legislação e cláusulas contratuais ( ) Requerimentos de treinamento em segurança da informação aos colaboradores da empresa ( ) Detecção e prevenção de vírus e software malicioso ( ) Gestão da continuidade do negócio ( ) Conseqüências da violação da política de segurança (OLIVA, 2003)
Segurança da Informação e TI	
Controles de segurança	A política de segurança da informação explicita quais controles e procedimentos de segurança efetivos devem ser incorporados aos sistemas? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Ciclo de vida dos sistemas	De que forma a segurança da informação faz parte do ciclo de vida dos sistemas? Você considera este fator um ponto forte ou fraco? (BERNARDES e MOREIRA, 2005)
Projetos de TI como ameaça	Cada projeto de TI é avaliado para saber de que forma pode se constituir numa ameaça à segurança da informação? Você considera este fator um ponto forte ou fraco? (DOHERTY e FULFORD, 2005a)
Nível Operacional	
Segurança da Informação e Negócio	
Consciência da segurança da informação (usuários finais dos sistemas)	De que forma os usuários finais dos sistemas e são treinados no uso seguro dos mesmos? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Consciência da segurança da informação (clientes)	De que forma os clientes do banco são esclarecidos sobre o uso seguro dos recursos de TI colocados à sua disposição? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Relacionamento com usuários	A política de segurança da informação estabelece direitos, responsabilidades e limites dos usuários e terceirizados em relação ao uso dos sistemas de informação da organização? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Segurança da Informação e TI	
Documentação	A documentação do projeto e da operação dos sistemas existe e está atualizada? Todos os sistemas? Você considera este fator um ponto forte ou fraco? (O'BRIEN, 2001)
Critérios de aceitação	Existem critérios de aceitação para novos sistemas, atualizações e

	novas versões? São efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Controles	Existem controles de detecção, prevenção e recuperação para proteger contra incidentes de segurança? Existem procedimentos para a devida conscientização dos usuários? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Infra-estrutura	
Diferencial competitivo	Como ocorre o processo de avaliação de tecnologias de infra-estrutura? É um diferencial competitivo? (DAVENPORT, 1998)
Confiabilidade	Você considera a confiabilidade, segurança e estabilidade da infra-estrutura da sua empresa como um ponto forte ou fraco? Por quê? (BERNARDES e MOREIRA, 2005)
Métricas	Qual a sua avaliação da qualidade do sistema de métricas da infra-estrutura? Seus pontos fortes e fracos? (SWANSON ET AL., 2003)
Usuários dos sistemas	
Consciência da segurança da informação (usuários finais dos sistemas)	De que forma os usuários finais dos sistemas são treinados no uso seguro dos mesmos? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Consciência da segurança da informação (clientes)	De que forma os clientes do banco são esclarecidos sobre o uso seguro dos recursos de TI colocados à sua disposição? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)
Clientes do banco (terminais bancários/*internet banking*)	
Consciência da segurança da informação (clientes)	De que forma os clientes do banco são esclarecidos sobre o uso seguro dos recursos de TI colocados à sua disposição? Você considera este fator um ponto forte ou fraco? (ABNT, 2005)