SEGURANÇA DA INFORMAÇÃO EM BANCOS NO BRASIL, À LUZ DA ISO 17.799:2005 E DO ERM – *ENTERPRISE RISK MANAGEMENT*

Paulette Melo, Abner Netto e Sergio Crispim

Universidade Municipal de São Caetano do Sul
Rua Santo Antônio, 50 - São Caetano do Sul - SP - Brasil - CEP 09550-001

paulette.melo@gmail.com
abner@enygma.com.br
scrispim@uol.com.br

RESUMO

As organizações enfrentam desafios competitivos dinâmicos que têm mudado o padrão da concorrência. Neste novo contexto, a confiança dos consumidores tornou-se uma das mais importantes fontes de vantagem competitiva sustentável, dado que ela é valiosa e rara para o cliente, e de criação complexa e dispendiosa pela concorrência. Dentre os vários atributos associados à confiança, o risco é o mais proeminente. O risco operacional surge como o mais relevante, pois influencia a formação do resultado econômico e correlaciona-se com todos os demais tipos de risco. A gestão da segurança da informação emerge como importante determinante do risco operacional. Leis e normas internacionais têm sido promulgadas para maior confiabilidade ao tratamento das informações, como a *Sarbox*, em 2002, Coso II/ERM, em 2004, e a ISO 17.799:2005. Este estudo analisou a adequação à ISO 17.799:2005 por parte de três dentre os cinco maiores bancos de varejo no Brasil. Analisando 54 itens da norma, os resultados demonstram que os bancos não estão adequados à mesma em 18,5% dos itens investigados; estão parcialmente adequados em outros 14%, e adequados em 67,5%.

Palavras-chave: Segurança da Informação, ERM, ISO 17.799, TI, bancos.

ABSTRACT

The organizations face dynamic competitive challenges that have been changing the standard of competition and into this new concept, the customers' trust became one of the most competitive advantage maintainable sources provided that it's precious and rare for the customer and complex and expensive for the competitors. Among several attributes associated to the trust, the most prominent is the risk. The operational risk appears like the most important administration risk because it influences the formation's economic results and correlates itself with all the kinds of risks. The administration of the safety information emerges as decisive of the operational risk. In order to give larger reliability to the treatment of the information, laws and international norms have been promulgated, like SarbOx in 2002 and COSO II / ERM, besides ISO 17799:2005. This study analyzed three among five larger retail banks in Brazil and its adaptation to ISO 17799:2005. Analyzing 54 items of the norm, the results evidenced that the banks aren't adapted in 18,5% of the them, however, it's partially adapted in 14% and totally adapted in 67,5%.

Keywords: Security Information, ERM, ISO 17799, IT, Banks.

1. INTRODUÇÃO

No século XXI, as organizações enfrentam desafios competitivos dinâmicos. A economia global, na qual bens e serviços fluem com relativa liberdade entre as nações, pressiona constantemente o mercado, mudando os padrões da concorrência entre as empresas (HITT, 2005). A revolução tecnológica e a Internet, aliadas à grande intangibilidade do mundo do comércio eletrônico, mudaram completamente as expectativas das pessoas (COVEY, 2005). O tempo das transações foi incrivelmente reduzido, preços podem ser instantaneamente comparados, e os níveis de qualidade foram padronizados e certificados por meio das ISOs (MOREIRA, 1999).

Diante dessas mudanças, todo o mercado foi compelido a se reestruturar, pois a Tecnologia da Informação (TI) facilita o processo de entrada de novas empresas, mas também amplia e expõe os pontos fracos nos mercados onde as empresas existentes concorrem (LOBATO, 2000). Não bastassem tais mudanças, a Internet alterou ainda o modo pelo qual a administração estratégica é praticada em todos os tipos de negócios.

Hitt (2005) salientou que o principal componente para a competitividade em mercados globais consiste no desenvolvimento e na implementação de uma estratégia eficaz. As empresas usam o processo de administração estratégica para entender as forças que atuam sobre o mercado e para desenvolver vantagens competitivas. O desenvolvimento dessas vantagens tem uma magnitude maior do que tem sido historicamente percebido. Para estabelecer as vantagens competitivas, as empresas precisam identificar e determinar seu potencial de geração de recursos, capacidades e competências essenciais, e vinculá-los à sua própria habilidade de criar um processo sustentável.

O novo ambiente de negócios traz consigo também ameaças. Dentre as grandes ameaças do mundo globalizado, estão a difusão das inovações econômicas, os ajustes políticos e culturais delas decorrentes, e o ciclo de vida dos produtos, cada vez mais curto (DAVIS & MEYER, 1997). Os padrões de desempenho se tornaram muito importantes nos negócios globais: qualidade, custos, produtividade, prazos e fluxos de operações. Nesse sentido, vive-se num mercado que "cultua a eficiência e as vantagens competitivas" (SROUR, 2003), pois só elas garantirão a obtenção de retornos acima da média, fator crítico à sobrevivência empresarial neste século.

Ampliando o entendimento sobre a importância da sustentabilidade no novo ambiente de negócios, Slywotsky (1996) constatou que as estratégias de grande parte das empresas haviam sido definidas dando maior ênfase ao ambiente interno, ou seja, as ações eram focadas basicamente na gestão de custos e na gestão da qualidade total. Essa atuação de dentro para fora definia todas as dimensões da concepção de negócio das empresas, que acabavam fazendo escolhas, e não apenas avaliando dados. E a forma como essas escolhas eram feitas determinava a diferença entre o crescimento do valor, estagnação ou obsolescência econômica. No atual ambiente competitivo, entretanto, a estratégia precisa ser definida de fora para dentro, trazendo novos desafios e riscos. Nesse sentido, Zohar (2000) afirmou que é cada vez mais difícil para as empresas ter controle sobre sua eficácia e, assim, o processo de administração estratégica torna-se cada vez mais relevante (HITT, 2005), correspondendo a uma abordagem racional que direciona e capacita a empresa a responder eficazmente aos desafios do cenário competitivo do século XXI.

A confiança é, dentre outras, fonte destacada de vantagem competitiva para a empresa. Ela é valiosa e rara para o cliente; insubstituível e de criação dispendiosa pela concorrência (HITT, 2005). Dentre os vários atributos associados à confiança, o mais proeminente deles é o risco (a probabilidade de ocorrência de um evento adverso para uma determinada situação esperada). Para o autor, a gestão do risco é estratégica, pois influencia diretamente as capacidades e competências essenciais da empresa, com maior ênfase nos riscos administrativo e individual. Os riscos interagem com a realidade e são fatos na vida corporativa, uma vez que resultados incertos são reflexos de decisões gerenciais.

O aumento do ritmo e a profundidade das mudanças atuais implicam aumento generalizado do risco inerente ao modelo de negócio de todas as empresas, principalmente em instituições financeiras. Considerando-se o risco inerente a cada uma dessas vertentes e seus desdobramentos, os bancos, enquanto captadores e

provedores de recursos financeiros para a sociedade, acabam, por conseqüência, tendo seu nível de risco potencializado. Adicione-se como fator de ampliação de risco às instituições financeiras a facilidade com que o fluxo de capitais pode migrar, dentro e entre países, como decorrência da globalização e do desenvolvimento da TI.

Entendendo que, no atual cenário competitivo, a gestão do risco é estratégica, este trabalho tem por objetivo analisar como algumas importantes instituições financeiras (bancos) de varejo que operam no Brasil estão gerenciando seus riscos operacionais à luz da ISO 17.799:2005, norma internacional para a gestão da segurança da informação.

2. REFERENCIAL TEÓRICO

A mensuração de risco teve como pioneiro Henry Markowitz, que, em 1955, apresentou, em sua dissertação de mestrado, os primeiros modelos matemáticos para o cálculo do risco total de uma carteira de ativos. Seu modelo começou, a partir daí, paulatinamente a ser utilizado por economistas e bancos de investimento (LUCCHESI, 2005).

A administração do risco tem por diretiva que "riscos são uma opção, não um destino"; portanto, alocá-los, mitigá-los, controlá-los ou, simplesmente, evitá-los constitui decisão estratégica fundamental (REVISTA DO BNDES, 2005).

Os riscos podem ser divididos entre aqueles cuja origem é o ambiente interno da empresa e aqueles que se originam do ambiente externo; e as agências independentes de classificação de risco caracterizam-nos em riscos de negócios e riscos financeiros. As instituições financeiras reconhecem seis tipos de risco: crédito, mercado, operacional, legal, de liquidez e de imagem (REVISTA DO BNDES, 2005). Dentre estes, o risco operacional é o que mais influencia na formação do resultado econômico das instituições financeiras. Esse risco decorre da realização das operações, estando associado à qualidade dos controles internos. Por essa razão, o Comitê de Basiléia, criado em 1974 e formado pelos presidentes dos bancos centrais do grupo dos dez países mais ricos (G10), versando sobre supervisão bancária, estabeleceu a ênfase no gerenciamento de riscos das instituições financeiras definindo-os como risco de crédito, risco de mercado e risco operacional. Em 2004, esse comitê divulgou o Novo Acordo de Capital da Basiléia, conhecido como Basiléia II, recomendando sua implantação entre os finais de 2006 e 2007. Para esse comitê, "risco operacional é definido como o risco de perda resultante de pessoas, sistemas e processos internos inadequados ou deficientes, ou de eventos externos". Tal definição inclui o risco jurídico, excluindo o estratégico e de reputação (BIS, 2004). Fraudes praticadas por funcionários e falhas em processos e sistemas informatizados decorrem de estrutura organizacional inadequada, na qual o planejamento é deficiente, os procedimentos não têm uniformidade, ou há obsolescência em produtos e processos. Assim, o risco operacional correlaciona-se com todos os demais tipos de risco.

A fim de conferir maior confiabilidade às informações prestadas ao mercado, como também reduzir as fragilidades no mercado financeiro e de capitais, principalmente diante dos escândalos financeiros do inicio deste século, foi promulgada, em 2002, a Lei *Sarbanes-Oxley* ou *Sarbox*. Aplicável às grandes corporações com acesso ao mercado de capitais norte-americano, essa lei, composta por onze capítulos, versa, entre outras atribuições, sobre a responsabilidade corporativa e a divulgação de informações financeiras, responsabilizando pessoalmente os executivos pelas informações prestadas.

Nessa linha, a *Securities and Exchange Commission* – SEC divulgou o documento preparado pelo *Committee of Sponsoring Organizations of the Treadway Commission* – Coso, denominado Gerenciamento de Risco Empresarial – Estrutura Integrada (*Enterprise Risk Management – Integrated Framework* ou *ERM*), conhecido no mercado como Coso II ou ERM. No mercado dinâmico, as técnicas de avaliação de risco evoluíram de forma significativa, gerando novos paradigmas. Esse documento prevê a proatividade, não a reatividade anteriormente adotada na gestão dos riscos; a identificação de problemas nos processos, e não nas pessoas; e foco em controles internos mais abrangentes. Nesse documento, o ERM é definido como o "processo realizado por um comitê diretivo de uma empresa, suas gerências, seus funcionários, incluído na estratégia que a permeia, desenhado para identificar eventos que possam, potencialmente, afetar o desempenho da empresa, a fim de

monitorar os riscos e assegurar que estejam compatíveis com a propensão ao risco estabelecida, permitindo prover, com segurança razoável, o alcance dos objetivos" (CAS, 2004).

Considerando-se que pessoas e empresas tomam decisões baseadas em informações incompletas (HITT, 2005), que apresentam riscos e oportunidades, e como toda empresa deve gerar valor para os acionistas, o ERM capacita o corpo gerencial a administrar com eficácia os riscos envolvidos. O valor da empresa é maximizado quando a administração estabelece estratégias e objetivos que consideram um balanço adequado entre crescimento e metas de retorno e a gestão do risco, objetivando a melhor alocação de recursos para maximizar os resultados do negócio (REVISTA DO BNDES, 2005).

A fim de obter um entendimento comum do ambiente de negócios global, tomando conhecimento dos riscos que poderiam prejudicar uma empresa, as diretrizes elaboradas pelo Coso I, a *Sarbox* e o Coso II/ ERM definem como lidar com os controles internos. Essa estrutura assegura e melhora a eficácia e a eficiência das operações, a confiabilidade de seus relatórios financeiros, e viabiliza o cumprimento das leis e regulamentações (PWC, 2005). Tais estruturas são modelos, e têm que estar embasadas em ações concretas.

As estruturas de controles Coso consideram cinco componentes inter-relacionados: o ambiente de controles; a avaliação do risco; as atividades de controle; as informações e a comunicação; e o monitoramento (PWC, 2005). Entendendo-se que o ambiente de controle é base para todos os demais componentes, nele é que a gestão da segurança da informação se insere.

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. O objetivo da gestão da segurança da informação é preservar os ativos de informação. Os sistemas de gerenciamento da segurança da informação visarão sempre à confidencialidade, integridade e disponibilidade (CARUSO & STEFFEN 1999; SÊMOLA, 2003). A confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela. A integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não-autorizadas não possam modificá-la, adicioná-la ou removê-la. Já a disponibilidade garante que os autorizados a acessar a informação possam fazê-lo sempre que necessário.

Se a preservação da informação é vital para qualquer empresa, também o é, de forma exponencialmente maior, para as instituições financeiras, visto serem depositários do patrimônio dos clientes. Com o crescente aumento de ataques e incidentes de segurança reportados nos últimos anos, os bancos aumentaram vertiginosamente seus investimentos em TI. Dados divulgados pelo Comitê Gestor da Internet no Brasil – Cert.BR mostram que o número de incidentes de segurança motivados por falhas e vulnerabilidades de *software* a ataques externos, vírus, *hackers* etc., passou de 3,1 mil, em 1999, para 52,6 mil, em 2004. Houve, entre o final de 2002 e o primeiro trimestre de 2003, um aumento de 84% no número de ataques e incidentes de segurança (MESQUITA, 2003). Pesquisa mais recente do Cert.BR apontou um crescimento de 1.313%, no segundo trimestre de 2005, nas notificações associados a fraudes virtuais, se comparadas com o mesmo período de ano anterior (BANTEL, 2005).

A Federação Brasileira das Associações de Bancos – Febraban estima que as instituições financeiras destinem 10% de seu orçamento para TI (que somou 12 bilhões em 2004) à segurança de sistemas, enquanto gastos anuais com segurança patrimonial, como vigilantes e portas giratórias, são da ordem de 1 bilhão (SAITO, 2006). O mesmo artigo informa que 20% dos brasileiros, conforme pesquisa feita pela *Unisys* (o estudo entrevistou 6,5 mil pessoas, entre 18 e 60 anos), têm alta preocupação com fraudes pela Internet, o que coloca o Brasil na última posição no *ranking* de uso de *Internet banking* para transações bancárias, com 18% apenas de usuários *on-line*. O México lidera a lista, com 57%.

A fim de implementar e normatizar a atuação das organizações na gestão da segurança da informação, em 1989, o *Commercial Computer Security Center*, órgão ligado ao Departamento de Indústria e Comércio do Reino Unido, publicou a primeira versão do PD0003 – Código para Gerenciamento de Segurança da Informação. Em 1995, este código foi revisado e publicado como um *British Standard*, com a deno-

minação de BS 7.799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e no crescimento da segurança da informação. A BS 7.799 foi revisada e atualizada em 1999, com o acréscimo de novos controles, devido às novas necessidades de mercado, como o comércio eletrônico e a computação móvel, entre outros aspectos, sendo publicada como Parte 1, BS 7.799-1:1999. Devido ao interesse internacional em uma norma de segurança da informação, a BS 7.799-1:1999 foi submetida à ISO. Em dezembro de 2000, a Parte 1 BS 7.799-1:1999 foi publicada como norma internacional ISO/IEC 17.799:2000, após sua aprovação, em outubro, na reunião do Comitê Internacional de Normatização realizada em Tóquio – Japão (OLIVA & OLIVEIRA, 2003). Em 2001, a Associação Brasileira de Normas Técnicas – ABNT publicou a versão brasileira da ISO/IEC 17.799:2000, que ficou com a denominação de NBR/ISO 17.799 – Código de Prática para a Gestão da Segurança da Informação. Em setembro de 2005, a norma sofreu uma atualização, principalmente no item relativo a recursos humanos, e foi publicada no Brasil como ABNT NBR/ISO IEC 17.799:2005 (ASSOCIAÇÃO BRASILEIRAS DE NORMAS TÉCNICAS – ISO 17.799, 2005).

A norma ISO/IEC 17.799 define 127 controles que podem compor o escopo do sistema de gerência de segurança (*Information Security Management System – ISMS*), enfocando o processo sob o ponto de vista do negócio da empresa. A norma contém 11 seções de controles: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes da segurança da informação; gestão da continuidade do negócio; e conformidade (ASSOCIAÇÃO BRASILEIRAS DE NORMAS TÉCNICAS – ISO 17.799, 2005).

Devido à concentração das informações em uma organização, o crime por computador torna-se um aspecto de elevadas perdas e alto risco para uma empresa. De acordo com a pesquisa do Instituto de Peritos em Tecnologias Digitais e Telecomunicações (IPDI), o prejuízo causado por fraudes virtuais a bancos e administradores de cartões de créditos somou R$ 300 milhões, em 2005, no Brasil, valor 20% superior aos R$ 250 milhões registrados em 2004 (SAITO, 2006). Em outra pesquisa, 35% das empresas reconhecem que tiveram perdas financeiras decorrentes de ataques e invasões em seus sistemas de informação (MÓDULO, 2003). Contudo, o percentual de empresas que não conseguiram quantificar essas perdas diminuiu de 72%, em 2002, para 65%, em 2003. Em muitos casos, essas perdas podem ser diminuídas com a adoção de um processo de gestão de segurança, onde está incluída a política de segurança. A correta implantação de uma política de segurança pode ser resumida em três aspectos: redução da probabilidade de ocorrência; redução dos danos provocados por eventuais ocorrências; e criação de procedimentos para se recuperar de eventuais danos (CARUSO & STEFFEN, 1999).

3. METODOLOGIA

Trata-se de um estudo exploratório: a pesquisa foi realizada tendo como respondentes representativas instituições financeiras de varejo. Desenvolveu-se, a partir da ISO 17.799:2005, um questionário, que foi entregue ao responsável pela gestão da segurança da informação.

O questionário desenvolvido foi definido após consulta prévia aos respondentes. Como as informações pertinentes ao tema envolvem posicionamentos estratégicos dos bancos, e considerados os riscos de imagem decorrentes da exposição de dados sigilosos, optou-se pela criação de um questionário aberto. À pesquisa bibliográfica seguiu-se a pesquisa de campo junto aos três bancos. Foi feita também pesquisa documental sobre o tema, em *sites*, documentos e vídeos de cada um dos bancos.

Dos 127 controles que podem compor o escopo do sistema de gerência da segurança da informação, a presente pesquisa analisou 54, julgados mais relevantes pelos autores, dispondo-os em questionário composto por 61 perguntas e mais 31 subperguntas. O questionário foi aplicado e respondido por três dentre os cinco maiores bancos comerciais de varejo no Brasil. Dois desses bancos são nacionais em sua origem, e o outro, internacional. Conforme dados do Banco

Central com data-base de dezembro de 2004, estes três bancos, juntos, possuem mais de 24 milhões de clientes e 113.281 funcionários. Sua capilaridade de atendimento está distribuída entre 4.879 agências e 12.664 postos de serviço. Estes três bancos apresentam ativos totais de cerca de R$ 271 bilhões. Seus depósitos totais perfazem R$ 130 bilhões. Além dos depósitos, administram outros R$ 211 bilhões de recursos de terceiros (valores em reais referentes ao balanço de 2004, os demais dados estão atualizados até dezembro de 2005).

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Os dados foram analisados e discutidos dentro da ordem em que constam da ISO 17.799:2005. Para todos os bancos respondentes, houve clareza na definição sobre o que entendiam como segurança da informação. A proteção dos ativos de informação, integridade, disponibilidade e confidencialidade das informações das quais são proprietários foram citadas por todos.

Seguem a seguir quadros sobre todas as seções pesquisadas, na ordem em que estão discriminadas na ISO 17.799:2005. Comparadas as respostas dadas pelos gestores e as orientações contidas na norma, os autores classificaram a conformidade dos bancos à norma como adequada, inadequada ou parcialmente adequada.

Na gestão da política da segurança da informação, foram registradas as conseqüências das violações para o negócio, representadas por perdas financeiras ou desgastes na imagem da instituição junto ao mercado. Assim, nos três bancos, a alta direção está comprometida e dá apoio visível a todos os níveis gerenciais sobre o tema. Num desses bancos, o próprio presidente foi citado como participante dos principais comitês executivos sobre riscos operacionais.

Enquanto é nítido o comprometimento da alta direção com o tema, os demais colaboradores não demonstram, de acordo com as respostas, um entendimento abrangente do seu papel. Uma das principais recomendações da norma prevê a transferência constante de conhecimento, além de conscientização, treinamento e educação em segurança da informação, comunicando a política da segurança da informação através de toda a organização para os usuários. Para isso, os três bancos têm distribuído a todos os funcionários as diretrizes e normas sobre a política de segurança da informação, e promovido programas de treinamento. Entretanto, dois dos respondentes ratificaram que o processo de entendimento não é uniforme entre os funcionários, apesar de perceber-se um aumento gradativo dessas competências.

Observa-se também que tais políticas são revistas de forma totalmente diversa entre os respondentes. A ISO preceitua que haja análises críticas em intervalos planejados ou quando mudanças significativas ocorrerem. Assim, enquanto um dos bancos faz sua revisão anualmente e o outro faz readequações sempre que a área julgar necessárias, o banco B não soube precisar essa informação, alegando que, naquele momento, estavam readequando suas políticas e seus procedimentos.

Quadro 1: Política de segurança da informação

Seção: Política de segurança da informação			
Objetivo: prover uma orientação e o apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.			
	Banco A	**Banco B**	**Banco C**
Definição de segurança da informação	Adequado	Adequado	Adequado
Estrutura de controle e gerenciamento do risco	Adequado	Adequado	Adequado
Comprometimento da alta direção	Adequado	Adequado	Adequado
Distribuição de diretrizes e normas	Adequado	Adequado	Adequado
Entendimento por parte dos colaboradores	Adequado	**Parcial**	**Parcial**
Período de revisão	Adequado	**Inadequado**	Adequado

Quanto à organização da segurança da informação, as estruturas dos bancos diferem. Em dois bancos, há superintendentes como gestores responsáveis, enquanto o outro tem um gerente como gestor responsável pela segurança da informação. Em dois dos respondentes, há comitês específicos para gestão da segurança da informação, e em outro, não. Nos bancos onde existem esses comitês, os membros vêm de várias áreas da instituição, multidepartamentalizada. As três instituições financeiras investigadas informaram que se utilizam de consultorias especializadas em segurança da informação para dar suporte à análise de riscos e implantação de políticas de segurança.

Os bancos informaram que colaboradores, parceiros e empresas contratadas firmam acordos de confidencialidade e de não-divulgação de informações no momento da assinatura do contrato de trabalho ou de negócios. Os três bancos, dada a representatividade que possuem, foram unânimes em afirmar que participam de fóruns especializados em segurança da informação, como Comitês da Febraban, Comitê Gestor da Internet do Brasil e da *ISSA – Information Systems Security Association,* associação internacional mais reconhecida na área. Não houve unanimidade, porém, nas respostas envolvendo terceirizados. Em dois dos bancos, existem políticas para a atuação de terceiros na gestão da segurança da informação. Em outro, não há política específica, embora todos, contratualmente, reivindiquem processos de aderência dessas empresas às normas de cada um dos bancos. Fica clara a adequação parcial de dois dos bancos pesquisados.

No quesito segurança da informação no relacionamento com os clientes, as três instituições utilizam-se de acessos remotos e Internet, além das informações constantes nos contratos, para "falar com o cliente" sobre o item segurança.

Quadro 2: Organização da segurança de informação

Seção: Organização da segurança de informação			
Objetivo: gerenciar a segurança de informação dentro da organização.			
	Banco A	**Banco B**	**Banco C**
Estrutura de gerenciamento estabelecida	**Parcial**	Adequado	Adequado
Coordenação da segurança de informação	Adequado	**Parcial**	Adequado
Existência de comitê da segurança	**Inadequado**	Adequado	Adequado
Gestor de segurança nas agências	Gerente Agência	Gestor da da Segurança	Gerente e Gerente Adm.
Consultoria especializada em segurança	Adequado	Adequado	Adequado
Acordos de confidencialidade	Adequado	Adequado	Adequado
Contato com autoridades em caso de incidentes	Adequado	Adequado	Adequado
Contato com grupos especiais	Adequado	Adequado	Adequado
Acordos com terceiros	Adequado	**Parcial**	**Inadequado**
Relacionamento com o cliente	Adequado	Adequado	Adequado

Quadro 3: Gestão de ativos

Seção: Gestão de ativos			
Objetivo: alcançar e manter a proteção adequada dos ativos da organização.			
	Banco A	**Banco B**	**Banco C**
Inventário dos ativos	Adequado	Adequado	Adequado
Regras para uso da Internet, *e-mail* etc.	Adequado	Adequado	Adequado
Classificação da informação	Adequado	**Inadequado**	**Inadequado**

A fim de inventariar os ativos da informação e seus proprietários, dois dos bancos pesquisados transferem para a área de TI a implementação desses sistemas de inventário. Num dos bancos, os ativos são mapeados com a descrição de seus responsáveis, e cada sistema ou banco de dados está associado a um proprietário.

Respondendo ainda sobre como classificavam as informações dentro da gestão dos ativos, dois bancos não possuíam nenhum critério para indicar a necessidade, as prioridades e o nível esperado de proteção quando do tratamento da informação, conforme recomenda a norma. No outro, em contrapartida, os métodos de classificação e tratamento de informações estão estabelecidos em uma política (manual de instruções) que determina e ensina o colaborador a classificar e rotular informações do banco ou dos clientes.

É consenso entre todos os bancos que, no momento da contratação, os colaboradores tomem ciência da política de segurança da informação, por escrito. Todos afirmaram que são feitas verificações das informações constantes no currículo dos novos colaboradores; em um deles, existe um processo de *background checking*, baseado nas práticas de mercado e nos aspectos que as leis brasileiras permitem que sejam avaliados. Os treinamentos em segurança da informação diferem de instituição para instituição. Enquanto o banco A, após a contratação dos funcionários, inclui o tema em seu "curso de integração", outro treina através de palestras e cursos a distância, e o banco C faz campanhas de *endomarketing*, vídeos, curso via *Web* etc.

A ISO recomenda que exista um processo disciplinar formal para os funcionários que tenham cometido violação da segurança da informação, considerando a natureza, a gravidade da violação e o seu impacto no negócio, entre outros fatores. Quando funcionários dos bancos pesquisados cometem alguma violação da segurança da informação, dois dos bancos conduzem o processo de acompanhamento e investigação disciplinar formal que é registrado em seus sistemas. O outro respondente afirmou que os processos disciplinares são conduzidos pelo RH, de acordo com a legislação trabalhista. Todos os bancos investigados têm procedimentos previstos quando da demissão ou troca de função do funcionário. Há bloqueio e suspensão ou readequação das senhas de acesso.

A segurança física e do ambiente está adequada. Todos os bancos têm controles de acesso predefinidos, com leitores de controles, caso necessária a permanência de "agentes patrimoniais" ou do gestor da área de acesso restrito. Em relação aos equipamentos usados fora das dependências do banco, ou controles sobre equipamentos para descarte ou remoção, houve unanimidade nas respostas dos bancos, com total aderência à ISO 17.799:2005.

No gerenciamento das operações e comunicações, todos os bancos mantêm documentadas as atividades de sistemas associadas a recursos de processamento e comunicação de informações. Um dos bancos utiliza uma ferramenta de *workflow* para esse registro. Quando ocorre alguma mudança em equipamentos, *software*

Quadro 4: Segurança em recursos humanos

Seção: Segurança em recursos humanos			
Objetivo: assegurar que funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de roubos, fraudes ou mau uso de recurso.			
	Banco A	Banco B	Banco C
Responsabilidades antes da contratação	Adequado	Adequado	Adequado
Seleção	Adequado	Adequado	Adequado
Documento com termos e condições de segurança	Adequado	Adequado	Adequado
Conscientização, educação e treinamento em segurança	Adequado	Adequado	Adequado
Processo disciplinar – sanções	Adequado	Adequado	**Inadequado**
Encerramento ou mudança na contratação	Adequado	Adequado	Adequado

ou procedimentos esses são registrados, porém, no banco C, esse processo não é auditável e, em outro, existe uma política e um comitê para aprovação dessas mudanças.

Há ambientes de desenvolvimento segregados em testes e produção, e somente após a validação dos testes é que o sistema entra em produção, conforme recomenda a norma. Em dois bancos pesquisados, a área de gestão de mudanças coordena esse processo.

Os controles utilizados para o monitoramento e a análise crítica de serviços terceirizados não dispensam a presença de representantes do próprio banco, alocados fisicamente nos locais onde os serviços são prestados. Além desses, há os controles internos das próprias empresas constantes no contrato efetivado.

A fim de identificar problemas em sistemas e documentar sua instalação, um dos bancos pesquisados adota a metodologia CMM (*Capability Maturity Model for Software*), que possui diretrizes e processos para cada etapa do desenvolvimento e manutenção de sistemas. Os outros dois bancos possuem métodos internos próprios, porém todos dispõem de um documento formal para aceitação e implantação de novos sistemas.

Para prevenir a entrada de códigos maliciosos (vírus, *worms*, *trojans*), todos os bancos utilizam-se de antivírus, porém somente dois desses bancos citaram outras ferramentas, como *IDS*, *antiSpam* e limitação à navegação. Somente um dos bancos possui um TRI – time de resposta a incidentes como forma de medida reativa, e outro banco citou o trabalho de conscientização alertando os colaboradores, conforme pede a norma.

Quadro 5: Segurança física e do ambiente

Seção: Segurança física e do ambiente			
Objetivo: prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização.			
	Banco A	**Banco B**	**Banco C**
Controle de entrada física	Adequado	Adequado	Adequado
Segurança em escritórios, salas e instalações	Adequado	Adequado	Adequado
Segurança de equipamentos	Adequado	Adequado	Adequado
Descarte ou remoção de equipamentos ou *software*	Adequado	Adequado	Adequado

Quadro 6: Gerenciamento das operações e comunicações

Seção: Gerenciamento das operações e comunicações			
Objetivo: garantir a operação segura e correta dos recursos de processamento da informação.			
	Banco A	**Banco B**	**Banco C**
Procedimentos e responsabilidades operacionais	Adequado	Adequado	Adequado
Gestão de mudanças – registro de auditoria	Adequado	Adequado	**Inadequado**
Segregação de funções de desenvolvimento	Adequado	Adequado	Adequado
Gerenciamento de serviços terceirizados	Adequado	Adequado	Adequado
Aceitação de sistemas	Adequado	Adequado	Adequado
Proteção contra códigos maliciosos (vírus, *worms, trojans*)	Adequado	Adequado	Adequado
Cópia de segurança (*back-up*)	Adequado	**Parcial**	Adequado
Segurança de redes	Adequado	Adequado	Adequado
Gerenciamento de mídias removíveis	Adequado	Adequado	Adequado
Segurança na troca de informações	Adequado	Adequado	Adequado
Monitoramento de atividades não-autorizadas	Adequado	Adequado	Adequado

Quando à política de cópias de segurança, dois bancos cumprem o que pede a norma, porém o terceiro banco não soube dar informações precisas sobre o processo de cópias de segurança. Quanto ao descarte de mídias antigas, todos os bancos possuem procedimentos formais. Para segurança dos serviços de rede, todos os bancos utilizam ferramentas que visam a proteger a comunicação, como o uso de criptografia e chaves de segurança. Dois bancos disseram possuir um TRI – time de resposta a incidentes de segurança, que monitora e audita eventos envolvendo riscos à segurança dos serviços de rede; um dos bancos citou somente o uso da ferramenta *IDS* (*Intrusion Detection System*).

No item da norma ISO 17.799:2005 sobre controle de acessos, todos os pesquisados alegaram possuir política de controle de acesso e direitos de cada usuário formalmente implantado, sendo que, em um dos bancos, essa política faz parte da própria política de segurança da informação. No item sobre gerenciamento dos direitos e senha dos usuários, cada banco ofereceu uma resposta diferente, de acordo com sua própria gestão. Um dos bancos pesquisados possui uma área específica para esse gerenciamento, enquanto outro alegou que cada sistema tem seu método específico de configuração de senhas e direitos, e, por último, uma das instituições citou a combinação de *softwares* específicos, produzidos internamente para esse fim.

O item "aquisição, desenvolvimento e manutenção de sistemas de informação", que trata da segurança de sistemas de informação, foi apresentado aos pesquisados por intermédio de três questões: a instalação de *softwares*, a segurança do código-fonte e as medidas tomadas no caso da descoberta de uma vulnerabilidade em um *software*. Na questão sobre instalação de *softwares*, todos os bancos responderam que há uma área interna responsável por esse processo.

Na questão sobre a segurança de códigos-fonte, dois bancos implementam-na segundo a norma. Um dos bancos pesquisados afirmou não ter conhecimento sobre como é feito esse processo. Uma vez descoberta qualquer vulnerabilidade em um *software* dentro da organização, os três bancos atuam imediatamente, conforme a ISO 17.799. Dois dos bancos possuem um grupo de respostas a incidentes que existem formalmente e que emitem alertas sobre casos. Um dos bancos informou que, nos últimos dois anos, mais de 400 alertas foram emitidos.

Dois dos bancos investigados possuem uma equipe de respostas a incidentes, sendo que, em um deles, essa área é reconhecida pelo Cert-BR, que trata de todos os incidentes ocorridos, atendendo via *e-mail* e tendo processos formais de registro. O outro banco também possui processos formais de registro, porém isso se dá por meio de uma central de atendimento via telefone ou *e-mail*, o que não ficou claramente explícito.

Quadro 7: Controle de acesso

Seção: Controle de acesso			
Objetivo: controlar acesso à informação.			
	Banco A	**Banco B**	**Banco C**
Políticas de controle de acesso	Adequado	Adequado	Adequado
Gerenciamento de acesso do usuário	Adequado	Adequado	Adequado

Quadro 8: Aquisição, desenvolvimento e manutenção de sistemas de informação

Seção: Aquisição, desenvolvimento e manutenção de sistemas de informação			
Objetivo: garantir que segurança é parte integrante de sistemas de informação.			
	Banco A	**Banco B**	**Banco C**
Controle de *softwares* operacionais	Adequado	Adequado	Adequado
Acesso ao código-fonte de programas	Adequado	**Inadequado**	Adequado
Gestão de vulnerabilidades técnicas	Adequado	Adequado	Adequado

Perguntados sobre os mecanismos estabelecidos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados, somente um banco alegou possuir quantificação de custos para serem apresentados à vice-presidência; um deles não respondeu à questão e o outro controla somente quantidades.

Com o objetivo de garantir a continuidade do negócio, todos os bancos possuem planos de contingência e continuidade do negócio, conforme respostas. Chamou a atenção a informação de um deles, que alegou possuir *back-up site* (local geograficamente distinto, onde existem cópias de todos os dados e instalações originais, a fim de prover a continuidade do negócio, caso ocorra algum desastre físico).

O último quesito da norma é a conformidade. No questionário apresentado, foram abordadas seis perguntas sobre o assunto. Na primeira pergunta sobre conformidade, todos os bancos afirmaram estar em conformidade com a norma, pois possuem controles internos ou termo de compromisso sobre o tema.

Tratando-se da proteção de registros importantes quanto à perda ou destruição, um dos bancos mantém essas informações em local seguro; outro possui controles internos que decorrem de sua própria política de segurança para esse tratamento. Apenas um dos bancos alegou a aderência à *Sarbox (Sarbanes-Oxley*), que cobre esse item.

Quando perguntados sobre a existência de uma política implementada a respeito da privacidade e da proteção de dados da organização, e sua forma de divul-

Quadro 9: Gestão de incidentes de segurança da informação

Seção: Gestão de incidentes de segurança da informação			
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes da segurança da informação.			
	Banco A	**Banco B**	**Banco C**
Responsabilidades e procedimentos	Adequado	Adequado	Adequado
Coleta de evidências	**Parcial**	Adequado	**Inadequado**

Quadro 10: Gestão da continuidade do negócio

Seção: Gestão da continuidade do negócio			
Objetivo: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.			
	Banco A	**Banco B**	**Banco C**
Continuidade de negócios e análise/avaliação de riscos	Adequado	Adequado	Adequado

Quadro 11: Conformidade

Seção: Conformidade			
Objetivo: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.			
	Banco A	**Banco B**	**Banco C**
Conformidade com requisitos legais	Adequado	Adequado	Adequado
Proteção de registros organizacionais	Adequado	Adequado	Adequado
Privacidade e informações pessoais	Adequado	**Inadequado**	Adequado
Mau uso de recursos de processamento da informação	Adequado	Adequado	Adequado
Conformidade com as políticas e normas da segurança da informação	Adequado	**Parcial**	Adequado
Verificação da conformidade técnica	Adequado	Adequado	Adequado

gação, dois bancos a têm, sendo que um deles divulga-a em seu *site* na Internet. O outro pesquisado desconhece tal política, evidenciando sua não-conformidade à norma.

Todos os funcionários, fornecedores e terceiros são advertidos sobre as penalidades existentes, caso ocorram abusos ou maus usos dos acessos permitidos. Um dos bancos evidenciou existir, para funcionários, um código de ética e, para fornecedores e terceiros, a aplicação unicamente das cláusulas contratuais.

Sobre a existência de mecanismos implementados para garantir que gerentes analisem a conformidade do processamento da informação dentro da sua área de responsabilidade com as políticas de segurança, dois bancos confirmaram-na como existente e implementada; o outro afirmou que ainda está em fase de implementação.

Para a aplicação de testes de invasão e avaliação de vulnerabilidades, todos os bancos possuem equipes internas preparadas, que atuam em conjunto com uma consultoria externa. Um dos bancos afirmou que opera, hoje, somente com consultoria externa, porém estão em processo de implantação da mudança que envolverá seu pessoal interno.

Além das questões referentes aos 11 quesitos da norma ISO 17.799:2005, foram incluídas, ao final do formulário, quatro questões relativas ao alinhamento estratégico do banco e à segurança da informação. Todos os gestores consideram que a gestão da segurança da informação está alinhada com o planejamento estratégico de suas instituições, e que isso representa vantagem competitiva sobre seus concorrentes. Quanto à certificação da norma ISO 17.799:2005, dois gestores acreditam que pode representar vantagem competitiva pelos menos nesse primeiro momento; o outro citou outras certificações como mais importantes: **Base I e II** e ***Sarbox***.

5. CONSIDERAÇÕES FINAIS

A ISO 17.799:2005 estabelece diretrizes para iniciar, implementar, manter e melhorar a gestão da segurança da informação nas organizações, além de prover diretrizes gerais geralmente aceitas sobre as metas para a gestão da segurança da informação. Os bancos mais adequados às normas da ISO 17.799:2005 conferem maior confiança às suas atividades interorganizacionais, capacitando-se a obter maiores vantagens competitivas.

Como a segurança da informação é assunto de importância estratégica, houve adequação parcial a apenas oito dos itens, o que corresponde a 14% dos itens pesquisados. Tal adequação parcial aparece nos seguintes temas: entendimento da política por parte dos colaboradores, coordenação da segurança da informação, acordos com terceiros, existência de cópias de segurança, coleta de evidências e conformidade às políticas e normas de segurança da informação.

Chama a atenção a total inadequação a dez itens, que correspondem a 18,5% dos itens pesquisados. As inadequações demonstram as seguintes vulnerabilidades em políticas e controles: não há período predefinido para a revisão das políticas da segurança informação; o comitê de segurança da informação não está padronizado; não há acordos com terceiros definidos com o detalhamento que a norma recomenda; falta classificação correta da informação; há processos disciplinares e sanções não-adequados à norma; há carência de registros de auditoria na gestão das mudanças; não houve clareza no acesso correto ao código-fonte dos programas; não há coleta adequada das evidências na gestão de incidentes; e é insuficiente a privacidade das informações pessoais.

A maior incidência de inadequação à norma ocorre na seção Organizando a Segurança da Informação, com duas inadequações para dez itens pesquisados, correspondendo a 20%. Observa-se, ainda, que foi registrada adequação total à norma nas seções de Segurança Física e do Ambiente, Controle de Acesso e Gestão da Continuidade do Negócio.

Dos dados analisados, ressalta-se que, dada a velocidade das mudanças impostas pelo mercado, as políticas de segurança da informação também deveriam sofrer revisões predefinidas, de cuja carência podem decorrer os demais problemas. Esta pesquisa demonstrou que cada banco faz revisões quando julga necessário. O presente trabalho aferiu também que questões relativas à segurança da informação são comunicadas aos clientes apenas por acesso remoto, o que pode ser considerado um procedimento inadequado, dada à complexidade do tema. Uma comunicação formal e

objetiva poderia consolidar a segurança da informação como vantagem competitiva.

Em relação ao treinamento dos funcionários, os procedimentos dos três bancos são muito diferentes, e talvez fosse conveniente que a Febraban estabelecesse alguns critérios padronizados de treinamento sobre segurança da informação.

Depreende-se, a partir dos dados analisados, que, a despeito de todo o controle relativo à segurança da informação nas instituições financeiras, há vulnerabilidade na sua relação com empresas coligadas, fornecedores e terceiros. Estas se constituem nas áreas de maior fragilidade na gestão da segurança da informação nos bancos pesquisados. A falta de política previamente definida para cada caso permite a existência de colaboradores-terceiros não totalmente envolvidos com a gestão da segurança da informação. Não houve também consenso quanto à transferência de riscos para as demais empresas do conglomerado, como seguradoras e fornecedores. Por força das determinações do Acordo de Basiléia, o conglomerado aprovisiona recursos para a cobertura dos riscos, porém a gestão da segurança da informação não interage diretamente com as demais empresas do grupo. Fornecedores e parceiros compartilham apenas parcialmente das responsabilidades sobre riscos identificados que fazem parte de seus negócios.

A despeito de os bancos analisados não estarem 100% adequados à ISO 17.799:2005, pode-se considerar que a aderência às suas recomendações é bastante elevada, conferindo maior competitividade e redução do risco operacional inerente aos negócios destas instituições.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ISO 17.799. ABNT NBR ISO/IEC 17.799:2005*. Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BANTEL, Guilherme. "Fraudes virtuais crescem 1.313% no Brasil". *IDG Now*: 08/07/2005, às 12h14. Disponível em <http://www.idgnow.uol.com.br>. Acesso em: 08/07/2005.

BEAL, Adriana. *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas, 2005.

BIS – BANK FOR INTERNATIONAL SETTLEMENTS. Disponível em <http://www.bis.org>.

CARUSO, Carlos A.A..& STEFFEN, Flávio Deny. *Segurança em Informática e de Informações***.** São Paulo: Editora Senac São Paulo, 1999.

CAS – CASUALTY ACTUARIAL SOCIETY. "ERM – *Enterprise Risk Management*" – 2004. Disponível em <http://www.casact.org/coneduc/erm/2004>. Acesso em: 20/12/2005.

COVEY, Stephen R . *O 8º hábito: da eficácia à grandeza***.** São Paulo: Campus, 2005.

DAVIS & MEYER. *Blur: a velocidade da mudança na economia integrada*. Rio de Janeiro: Campus, 1999.

HITT, Michael A.; IRELAND, R. Duane & HOSKISSON, Robert E. *Administração estratégica***.** São Paulo: Pioneira Thomson Learning, 2005.

LUCCHESI, Cristiane P. "A Beleza dos Números". *Valor Econômico*, 19 de agosto de 2005.

LOBATO, David Menezes. *Administração estratégica: uma visão orientada para a busca de vantagens competitivas*. Rio de Janeiro: Editoração, 2000.

MESQUITA, Renata. "Ataques *hackers* triplicaram no 1º trimestre"**.** Plantão Info: 30/04/2003, às 09h49. Disponível em <http://www.infoexame.com.br>.

MÓDULO. 9ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro: outubro, 2003. Disponível em <http://www.modulo.com.br>.

MOREIRA, Joaquim Manhães. *A ética empresarial no Brasil*. São Paulo: Pioneira, 1999.

OLIVA, Rodrigo Polydoro & OLIVEIRA, Mírian. "Elaboração, implantação e manutenção de política de segurança por empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO 17.799". Anpad, 2003.

REFERÊNCIAS BIBLIOGRÁFICAS

PWC – PRICE WATERHOUSE COOPER. Disponível em <http://www.pwc.com>. Acesso em: 21/12/2005.

REVISTA DO BNDES. Rio de Janeiro, volume 12, n. 24, p. 149-168, dezembro, 2005.

SAITO, Ana Carolina. "Banco perde mais com fraude virtual" *Gazeta Mercantil*, São Paulo, 11 de janeiro de 2006, C-1.

SÊMOLA, Marcos. *Gestão da Segurança da Informação: uma visão executiva*. Rio de Janeiro: Campus, 2003.

SLYWOTSKY, Adrian J. "*Value migration: How to think several moves ahead of the competition*". *Harvard Business School Press*, 1996.

SROUR, Robert Henry. *Ética empresarial: a gestão da reputação*. Rio de Janeiro: Campus, 2003.

ZOHAR, Danah. *QS: Inteligência espiritual – o "Q" que faz a diferença***.** Rio de Janeiro: Record, 2002.