RISCO OPERACIONAL NO COMPARTILHAMENTO DE TERMINAIS DE AUTOATENDIMENTO (ATM)

TATIANA GUIMARÃES CHASSOT

Universidade do Vale do Rio dos Sinos - UNISINOS

ROSANE MACHADO MACIEL

Universidade do Vale do Rio dos Sinos – UNISINOS

MARIA CECILIA DA SILVA BRUM

Universidade do Vale do Rio dos Sinos – UNISINOS

ADOLFO ALBERTO VANTI

Universidade do Vale do Rio dos Sinos – UNISINOS

RESUMO

Gerentes, vendedores e negociantes iniciam transações que resultam em riscos de mercado e de crédito para a empresa, enquanto que gerentes de operações empreendem ações que produzem riscos operacionais. Dos quatro tipos de risco (risco de mercado, risco de liquidez, risco operacional e risco de crédito) muito enfrentados pelas empresas e para os quais alocam capitais, a gestão de riscos operacionais é a menos adiantada afirma Marshall (2002). Este trabalho analisou risco operacional em serviço de compartilhamento de terminais de autoatendimento em um Banco através da operação de saques. O foco da análise deste tipo de risco considerou sistemas utilizados para o registro, contabilização, rateio e eventuais ajustes. Foi adotada a metodologia de estudo de caso único, exploratório com análises qualitativas. Conclui-se que a instituição estudada atende à legislação vigente e busca melhoria contínua em seus processos que envolvem riscos operacionais, monitorando-os através de conciliação contábil, e pelo acompanhamento da evolução das contas do risco. São aplicados planos de ação pela área de gestão de processos e o controle é realizado pela Gerência de Risco Operacional do Banco estudado.

Palavras-chave: Risco Operacional. Terminais de autoatendimento (ATM). Gestão de riscos

1. INTRODUÇÃO

O uso da tecnologia como apoio ao processo organizacional tem proporcionado oportunidades e incrementos na competitividade das organizações. No setor bancário este uso tem gerado uma interação cada vez mais efetiva entre bancos e clientes, acarretando no uso de sistemas e no controle dos processos, uma vez que uma falha nas operações pode emergir em perdas significativas.

Conforme Crouhy, Galai e Mark (2007) o *Basel Committee*[1] emergiu como a entidade mais próxima do que o setor bancário internacional tem como regulador. Foi criado para promover segurança e solidez no sistema financeiro, aprimorar a equidade competitiva e aplicar uma abordagem mais abrangente aos riscos. O comitê da Basiléia entende que a gestão do risco operacional é composta pelas etapas de identificação, avaliação, monitoramento e controle/mitigação do risco e comunicação (COIMBRA, 2006; ALVES, 2005 e CASTRO, 2009). A gestão de riscos operacionais pode contribuir com a responsabilidade social corporativa, através do incentivo ao comportamento ético e socialmente responsável (CROUHY, GALAI e MARK, 2007, MACHADO, 2012 e COIMBRA, 2006).

Com a análise do risco operacional dos saques utilizando o serviço de compartilhamento de terminais de autoatendimento em um Banco, este trabalho verificou tais tipos de riscos adotando uma metodologia de estudo de caso com análises qualitativas. Na continuidade é apresentada a Fundamentação Teórica para logo descrever a metodologia e finalmente os resultados, conclusão e referências bibliográficas utilizadas.

[1] Comitê da Basiléia

2. FUNDAMENTAÇÃO TEÓRICA

2.1 RISCO OPERACIONAL

Através dos conceitos abordados na matéria, neste estudo foram adotadas como base legal para a operacionalização do controle de risco as seguintes regulamentações: internacionalmente o Novo Acordo de Capitais da Basileia (Basileia II) e nacionalmente a Resolução Normativa 3.380 do Banco Central do Brasil. A partir das alterações propostas pelo Basiléia II o Risco passa a contar às perdas que envolverem erros de funcionários, falhas de computador, documentações irregulares ou fraudes. (BANZAS, 2005).

"O risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos" (COSO, 2007, p.22). Para Dionee (2013), uma abordagem de gestão integrada dos riscos deve avaliar, controlar e monitorar todos os riscos e as suas dependências para que a empresa está exposta.

Em muitos casos, faz-se necessário o detalhamento de categorias de riscos operacionais em subcategorias, de modo a refletir os eventos de risco operacional que realmente podem ocorrer em uma organização (ELO GROUP, 2007). Em geral, um risco genuíno é uma combinação de frequência ou a probabilidade de um evento e as suas consequências, a qual é geralmente negativa (Dionee, 2013).

Para o banco foco do estudo a política de gerenciamento do risco operacional constitui um conjunto de princípios, procedimentos e instrumentos que proporcionam uma permanente adequação dos dispositivos de monitoramento, controle e mitigação. As responsabilidades dos envolvidos são definidas de acordo com a natureza e complexidade dos produtos, serviços, atividades (NBC TA 610), processos e sistemas (CFC, 2010 e ELO GROUP, 2007). As atividades de gerenciamento do risco operacional no banco e empresas controladas estão sob a responsabilidade da Superintendência de Controles Internos, Compliance[2] e Risco Operacional, vinculada diretamente à Presidência Executiva.

O processo de avaliação dos riscos se preocupa com a identificação, análise e avaliação dos riscos, refere-se ao mapeamento das diversas atividades. São ferramentas para monitorar, relatar, medir e determinar as tolerâncias e controlar/mitigar o risco operacional (ALVES, 2005, PEDOTE, 2002, HORI, 2003, MARSHALL, 2002 e MACHADO, 2012). "A questão de gestão do risco organizacional está intrinsecamente ligada à forma como as instituições financeiras se organizam estruturalmente" (PEDOTE, 2002, p. 11).

Segundo Brito (2007) e Attie (2011) a gestão de risco operacional em instituições financeiras se intensifica devido a dois principais motivos: demanda por alocação de capital específico para risco operacional e exigência de mercado para otimização de controles internos em instituições financeiras. De acordo com Pedote (2002) e Attie (2011) o gerenciamento do risco operacional está na definição de medidas e controles que eliminem as ameaças. Para Brito (2007), reputação organizacional está relacionada com mercados e subordinada ao profissionalismo e a padrões de conduta de gestores.

2.2 OPERAÇÕES DE COMPARTILHAMENTO DE ATM

Na década de 80 foi criado o sistema de banco24Horas da Tecban, possibilitando diversas operações (compras, saques, consultas, contratação de empréstimos, e outras funções atuais dos cartões) com interação entre bancos. Posteriormente a Tecban tornou-se

[2] Observância; conformidade

independente e ampliou os serviços às redes bancárias interessadas nos produtos e serviços oferecidos pelo sistema de compartilhamento e Banco24Horas.

O serviço de compartilhamento de ATM está em operação desde o ano de 1998, contendo mais de 32 mil terminais de autoatendimento cadastrados e habilitados para o serviço de nove instituições financeiras diferentes que compartilham suas redes para seus clientes. Somando dezesseis instituições financeiras que são usuárias deste sistema, opera em média 6,3 milhões de transações/ano (TECBAN, 2014). Para Saunders (2007) os Caixas Eletrônicos (ATMs) permitem aos clientes acesso durante 24 horas a suas contas correntes. Esse acesso pode incluir o pagamento de contas, além de retiradas de dinheiro.

Segundo Lancelotti (2005) o compartilhamento de uma atividade pode resultar em uma vantagem competitiva sustentável, se a vantagem do ato de compartilhar for superior ao seu custo, desde que seja difícil para os concorrentes equipararem o compartilhamento. O autor complementa ainda que os bancos pioneiros do serviço Banco 24horas vivenciaram essa situação, uma vez que equipararam a relação entre concorrentes participantes do compartilhamento. Passaram a enfrentar uma desvantagem competitiva em relação aos bancos que criaram redes de autoatendimento proprietária.

O serviço de compartilhamento de redes permite que clientes de uma instituição financeira (banco emissor) utilizem terminais de autoatendimento de outra instituição financeira (rede proprietária) – Interligado à rede Banco24Horas (TECBAN, 2014). Uma possibilidade para os bancos reduzirem custos nos seus ATMs é permitir que as máquinas de autoatendimento fizessem depósitos sem envelopes.

De acordo com Lancelotti (2005) a decisão de investir nesse tipo de projeto com meios eletrônicos e compartilhados é uma decisão estratégica, mas que também passa por um enfoque mercadológico. Por esta razão é importante considerar que uma estratégia mercadológica afeta os serviços disponíveis como: saque, consulta de saldo, emissão de extratos, troca de senha e pagamentos (SOUZA, 2001).

Segundo a Tecban (2014) com o serviço de compartilhamento de ATMs as instituições financeiras emissoras obtém as vantagens de redução de custos, aumento da capilaridade, maior conveniência para seus clientes, baixo custo de implementação, aumento do número de pontos de atendimento e a cobertura no território nacional. Considerando dentre as estratégias específicas o compartilhamento é, sem dúvida, uma solução estratégica que pode colaborar para enquadrar os custos à política da empresa, que também pode constituir-se numa alternativa para a diferenciação, ou neutralizar uma diferenciação eliminando um aspecto negativo da empresa em relação aos concorrentes (LANCELOTTI, 2005).

De acordo com Souza (2001) manter uma rede própria de terminais de autoatendimento implica em altos investimentos. Uma maneira de minimizar estes gastos e ao mesmo tempo fornecer uma rede ampla para atendimento aos clientes é o compartilhamento das ATMs entre as instituições financeiras. As vantagens para a instituição financeira proprietária da rede é a rápida implementação do modelo técnico e de negócio, o baixo custo da infraestrutura já existente e receita adicional e também o aumento da produtividade do parque (TECBAN, 2014).

De acordo com Lancelotti (2005) empresas associam-se a outros agentes, para execução dos seus processos, como parceiros e soluções. A empresa exerce um controle da cadeia produtiva, subordinando às estratégias globais de seus agentes e outros do gênero, com um sistema flexível, descentralizado de informação e de integração.

Souza (2001, p. 13) então conceitua Rede Compartilhada.

> [...] podemos definir a Rede Compartilhada como a interligação de vários bancos conveniados, com o intuito de dar aos seus clientes uma opção maior de locais de acesso.

A TecBan (Tecnologia Bancária S.A.) é uma empresa especializada na gestão de redes de autoatendimento bancário, reconhecida pelos seus elevados índices de disponibilidade, qualidade e segurança (TECBAN, 2014) O principal foco da TecBan é atuar como a rede complementar dos bancos no relacionamento com seus clientes, possuindo quatro unidades de negócios: a Rede Banco24Horas, o ATMManager, o Compartilhamento de Redes e o Switch Interbancos (TECBAN, 2014).

Conforme Lancelotti (2005) o compartilhamento de uma rede de ATMs também é uma formação de aliança, para isso o autor recomenda a compreensão de que esse processo de valor parta da orientação da Cadeia de Valor (PORTER, 1990), sendo esta considerada um processo por meio do qual devem alinhar-se as várias atividades primárias e secundárias da empresa.

De acordo com Rodrigues (2012) a rede Tecban é formada por todos os saques crédito e débito efetuados pelos associados no Banco24Horas (caixa eletrônicos próprios da Tecban) e na Rede Compartilhada (caixas eletrônicos de outros bancos que possuem a logomarca da Tecban). Todos os saques, independentes se débito ou crédito, são pagos à Tecban no dia seguinte.

Na continuação é apresentada a metodologia utilizada nesse trabalho.

3. METODOLOGIA

Trata-se de uma pesquisa aplicada, com características qualitativas que foi aprofundada em um estudo de caso. Este foi elaborado em um banco, que possuem terminais de autoatendimento com *software* licenciado para o serviço de compartilhamento de ATM. Este serviço é viabilizado através da TECBAN que operacionaliza e intermedia as instituições financeiras, possibilitando a comunicação entre elas.

Como técnicas para coleta de dados foram utilizadas a observação participante, a pesquisa documental e as entrevistas semi-estruturadas. A coleta de dados através de entrevistas contemplou as seguintes etapas:

Seleção dos respondentes: para esta etapa foi considerada a atuação e vínculo do participante com os processos de gestão de risco, produto compartilhamento (Canais e TI), bem como o interesse e disponibilidade em participar da pesquisa.

Tabela 1: Características dos participantes

Cargo	Formação Acadêmica	Idade
Analista de canais de relacionamento	Administrador	26 anos
Analista de controles internos	Contador e Administrador	31 anos
Coordenador de gestão de mudanças de TI	Administrador	36 anos
Supervisor contábil	Contador	35 anos
Coordenador de prevenção a fraudes	Administrador	35 anos
Ouvidor	Administrador e Advogado	49 anos

Fonte: Dados da Pesquisa (2014).

Agendamento da entrevista: o agendamento do encontro deu-se através de trocas de e-mail e correspondência formal, convencionando o horário adequado aos participantes do encontro.

Elaboração do roteiro da entrevista: adotado o modelo de Yin (2010) para elaboração de questões conceituais, o roteiro fora elaborado através dos quesitos considerados mais importantes e adequados ao caso em estudo.

Aplicação da entrevista: deu-se preferência para entrevista pessoal, porém não se dispensou a entrevista por intermédio de encontro virtual através de Web Conferencia por Skype.

A técnica de análise de dados utilizado neste estudo foi a qualitativa, pois se baseou na observação de um caso específico sem a necessidade de quantificar os resultados (RICHARDSON *et al*., 2008).

A apresentação dos dados deste trabalho deu-se pela unificação das respostas apuradas nas entrevistas formulando conceitos únicos, bem como a análise documental de relatórios disponíveis (LAKATOS e MARCONI, 2007).

4. RESULTADO

4.1 Identificação dos riscos operacionais do Banco

O banco estudado possui uma área de gerenciamento de risco operacional (controles internos, *compliance* e risco operacional). A área de risco operacional do banco atua em duas frentes para identificação do risco (BACEN, 2006): com o mapeamento do risco no CAS, utilizando a metodologia *scope map*[3], com base nos saldos das contas contábeis para identificação e diagnóstico das principais exposições a falhas ou incorreções no que concerne ao risco operacional e nas agências, Centrais e UAs com seis matrizes de risco (1. acesso e cadastros; 2. conta corrente; 3. operações de crédito geral; 4. operações de crédito rural; 5. operações de crédito BNDES (Banco Nacional do Desenvolvimento); e 6. Depósitos a prazo e poupança). Também são coletados elementos de diagnóstico em outras fontes de informação, como relatórios de inconformidades, reportes de incidentes ou de auditorias internas e externas.

Em complemento, há a atuação das falhas no produto de compartilhamento de terminais de autoatendimento que atua de forma a identificar os tipos de falhas que podem ocorrer como a falta de comunicação com a instituição financeira de origem (risco de imagem), a falha na contagem de cédulas e o registro contábil correto. As informações podem ser trazidas após a ocorrência, pelo cliente através de contato com o atendimento Tecban, DiskTecBan, ou diretamente na Unidade de Atendimento (UA) onde efetuou a tentativa de saque. Desta forma é acionada a área de canais para a verificação perante a TecBan, na qual são analisadas as falhas na comunicação. A conciliação contábil atua na constatação de sobras de caixa e em última instância a visualização das imagens capturadas pelas câmeras de vídeo. Geralmente a área de risco não atua diretamente no produto.

Todo o ciclo de gerenciamento do risco operacional é suportado por ferramenta sistêmica – SAS EGRC (*statistical analysis system – enterprises: governance, risk and compliance*[4]), que integra as informações em tempo real, em todas as instâncias. Na mesma ferramenta vem sendo constituída e analisada uma base de perdas operacionais, por entidade.

Cada agência disponibiliza um analista que faz a verificação das perdas operacionais no SAP (*Systeme, Anwendungen und Produkte*[5]) e classifica cada perda nas aberturas por tipo de risco, em conformidade com a Resolução 3.380/06.

O relatório de canais é publicado no portal do banco, para acesso das agências, com periodicidade semanal, na área de *Business Intelligence*[6] (BI) cujo objetivo é a demonstração

[3] Mapa por escopo
[4] Sistema de análise estatística - empresas: governança, risco e conformidade.
[5] Sistemas, Aplicativos e Produtos
[6] Inteligência de negócio

de desempenho dos canais do banco no período informado, visualização em nível de UA, agência, central e visão geral do banco. As receitas das tarifas deste produto são calculadas através do volume das transações (transações vezes o valor da tarifa atual).

O recebimento das informações da TecBan de alterações das tarifas são compiladas e enviadas para a retaguarda efetuar a parametrização das mesmas no sistema. No sistema intranet de relatórios existe a possibilidade das agências emitirem o relatório das liquidações que são referentes aos repasses (recebimentos e pagamentos) da TECBAN, o sistema que faz esta interface é o SIGC (Sistema Integrado de Gestão de Cartões) sendo o relatório de liquidações gerado através do SGR (Sistema de Gestão de Redes) que por sua vez gera a agenda de pagamentos através do processamento dos arquivos que são recebidos da TECBAN com as informações sobre as transações. Após o repasse pelo SGR, as informações são integradas à contabilidade pelo SAP, o que é possível então, a geração de relatórios contábeis.

4.2 Análise dos principais riscos operacionais

O mapeamento das diversas atividades está relacionado com ferramentas para monitorar, relatar, medir e determinar as tolerâncias e controlar/mitigar o risco operacional (ALVES, 2005, PEDOTE, 2002, HORI, 2003 e MARSHALL, 2002). No banco o monitoramento é realizado através da conciliação contábil, e nela já são aprimorados os ajustes, comunicação e informação que constituem o processo de implementação, manutenção e divulgação destas etapas.

Semanalmente é emitido um relatório de inteligência organizacional disponível para acesso das agências através do portal, cujo objetivo é demonstrar o desempenho dos canais no período informado e as alterações de valores das tarifas são enviadas via CO.

Semestralmente são enviados COs com atualizações do detalhamento dos sub níveis das perdas, treinamentos e esclarecimento das políticas (papéis e responsáveis). O banco também possui a centralização de diversos processos na ferramenta *e-learning*, que possibilita o treinamento a distância de noventa por cento das atividades desempenhadas por colaboradores do banco, em seus diversos níveis e funções (ALVES, 2005).

O banco adquiriu no ano de 2013 equipamentos que impossibilitam fraudes de clonagem de cartão, usada por fraudadores numa sobreposição juntamente ao leitor de cartões que efetuam a cópia, bem como câmeras instaladas ao lado dos teclados dos ATMs para identificar a senha digitada pelo usuário no momento do saque ou consulta. Estes equipamentos (*anti-skimming*[7]) identificam a inserção destes dispositivos para fraude e emitem um alarme para a área de segurança patrimonial, que de imediato avaliam as necessidades para a remoção da sobreposição, bem como ativa os órgãos de segurança pública através de ocorrência policial. Como forma de recuperação destas perdas as agências possuem vínculo obrigatório ao Fundo Garantidor que conceitualmente é parte de uma ampla rede de proteção aos sistemas financeiros. Essa rede envolve, também, regulação prudencial, supervisão eficiente, legislação, práticas adequadas de gestão e metodologias adequadas de contabilidade e de transparência na divulgação de informações à população, como encontrado em Saunders (2007) e Bacen (2006).

[7] Anti-clonagem

4.3 Ações capazes de reduzir o risco operacional

Em geral bancos não segregam o tema risco operacional como uma atividade exclusiva da área de controles internos, *compliance* e risco operacional (PEDOTE, 2002, MARSHALL, 2002, HORI, 2003), mas como uma preocupação de todos no Sistema. Isso ocorre através do monitoramento e controle das alterações (ALVES, 2005) e transações, desde a agência, onde está o terminal compartilhado, da conciliação contábil do *cash dispenser* à conta transitória e conta do Banco onde fica a contabilização do recebimento dos saques efetuados no serviço de compartilhamento de ATM. A comunicação de erros, falhas, inconsistências são realizadas desde abertura de incidentes, para análise de causa raiz a e-mails para troca de informações como diferença de caixa inconsistente (COIMBRA, 2006, CASTRO).

A área de risco operacional atua de duas formas, a forma preventiva, emitindo e publicando as matrizes de risco, utilizando-se da segregação pelos tipos de risco, analisando os possíveis acontecimentos que poderiam gerar a perda e na identificação dos mesmos. E de forma detectiva, oferecendo a captura do registro contábil e posteriormente na atuação de prevenção de novas ocorrências.

Atendendo as exigências do Sistema de Pagamentos Brasileiro (SPB) o banco realiza testes semestralmente, conforme orienta o manual de segurança da RSFN[8] para certificação digital de mensageria. O plano de contingência e continuidade realiza testes sistêmicos para garantir a continuidade e integridade das atividades e uma resposta emergencial adequada. Baseado nos resultados do PRDTI (Planos de Recuperação de Desastres em TI), são realizadas melhorias nos planos para assegurar a eficácia da ativação dos sistemas no datacenter secundário e retorno ao datacenter primário.

Este procedimento, que ocorre semestralmente, visa atender, também, as exigências legais de conformidade à Resolução CMN 3.380/2006 e o Código de Serviços Qualificados da ANBIMA, as quais objetivam a implementação e testes de planos de contingência a serem adotados para assegurar condições de continuidade das atividades de negócio, limitando graves perdas decorrentes de risco operacional. Conseguinte aos testes de continuidade dos sistemas de informação são verificadas as mudanças necessárias para correções ou melhorias no funcionamento dos sistemas, requisições de mudança (RDM) são feitas através de especificações, testes e homologações.

Considerando trocas de funções, plano de contingência e estratégias que assegurem a continuidade das atividades conforme BACEN (2006) e MARSHALL (2002), a política adotada pelo Sistema da empresa estidada, estão estabelecidas na Política de Continuidade de Negócios e os princípios básicos em documentos na rede interna e BPA (*Business Process Analysis*[9]). Estes são publicados no Portal do Sistema com a estrutura necessária para garantir a resposta emergencial adequada, à recuperação, à restauração e aos níveis acordados de disponibilidade para os processos mais críticos da organização no caso de ocorrência de eventos que provoquem a interrupção dos seus serviços. Preserva, assim, os interesses de todas as partes envolvidas.

Políticas bem definidas constantes no Código de Ética, Código de Conduta em geral contribuem para o comportamento socialmente responsável. Ainda constitui o Comitê de auditoria, *Compliance* e Conduta, por avaliar e emitir parecer quanto aos padrões e procedimentos a serem adotados, para o atendimento de normas oficiais e internas e, apoiar nas definições dos padrões de conduta pessoal e profissional a serem observados no âmbito do

[8] Rede do Sistema Financeiro Nacional
[9] Análise de processos de negócio

Sistema, com periodicidade trimestral, de forma ordinária, e extraordinariamente quando necessário. Além disso, o banco tem como um dos principais valores o de colaboração e cooperação, identificado no dia-dia na interação entre as áreas.

A mitigação do risco operacional de saques utilizando o serviço de compartilhamento de terminais de autoatendimento pode ser conquistada (SOUZA, 2001) através de conciliação diária dos terminais e melhorias de sistema – controles – com um olhar garantindo que o sistema permanecerá em pleno funcionamento sem falhas por conta destas melhorias sistêmicas (RODRIGUES, 2012, TECBAN, 2014).

5. CONCLUSÃO

O banco estudado atende à legislação vigente e busca melhoria contínua em seus processos operacionais e na redução do risco operacional. A integração dos sistemas que atuam no processo de compartilhamento poderia ser melhor ajustada, perante a Tecban, no que se relaciona com as mudanças em parâmetros de trânsito de informações entre as instituições.

O banco monitora estes riscos através de conciliação contábil, buscando o acompanhamento também pela evolução das contas do risco, avalia a variação do risco operacional olhando para o mercado, comparando os diferentes riscos de outros bancos. Para alterações e implementações busca a devida comunicação através do portal interno de todo o Sistema do banco, e para o produto de compartilhamento de ATM existe uma página específica, cuja atualização é feita conforme a necessidade.

As ações capazes de reduzir o risco operacional são propostas de atividades diárias, acompanhamento, conciliação contábil através do monitoramento e controle das alterações, desde a agência à conta transitória e conta do Banco. A comunicação de erros, falhas, inconsistências são realizadas desde a abertura de incidentes até e-mails para troca de informações como diferença de caixa inconsistente, mesmo que a comunicação não ocorre para a Tecban.

Os testes dos sistemas são realizados semestralmente, em atendimento às legislações 3.380/06 do BACEN e ao Sistema de Pagamentos Brasileiro (SPB). O plano de contingência e continuidade realiza os testes sistêmicos para garantir a continuidade e integridade das atividades e uma resposta emergencial adequada. Baseado nos resultados do PRDTI, são realizadas adequações e melhorias nos planos para assegurar a eficácia da ativação dos sistemas.

São aplicados planos de ação pela área de gestão de processos, e o controle para o tratamento de riscos operacionais é realizado pela Gerência de Risco Operacional do Banco.

REFERÊNCIAS

ALVES, Carlos André de Melo. **A divulgação do risco operacional segundo recomendações do Comitê da Basiléia: estudo em bancos com carteira comercial no Brasil**. Dissertação (Mestrado em Administração). Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, 2005.

ATTIE, William. **Auditoria: conceitos e aplicações**. 6 ed. São Paulo: Atlas, 2011.

BACEN, Banco Central do Brasil. **Museu do Banco Central do Brasil**. 2014. Disponível em: <https://www.bcb.gov.br/?HISTCARTAO>. Acesso em: 22 mar. 2014.

_____. **RN 3.380, de 29/06/2006**. 2006. Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=res&ano=2006&numero=3380>. Acesso em: 22 mar. 2014.

_____. **Manual de Segurança da RSFN**. 2013. Disponível em: <http://www.bcb.gov.br/sfn/ced/manualdeseguran%C3%A7adarsfn-v32.pdf>. Acesso em: 03 mai. 2014.

BANZAS, M. S. **Governança corporativa no setor bancário: evolução recente no mercado brasileiro**. Dissertação (Mestrado em Administração). Instituto COPPEAD de Administração, Universidade Federal do Rio de Janeiro, 2005.

BRITO, Osias Santana. **Gestão de riscos: Uma abordagem orientada a Riscos Operacionais**. Ed. 1. São Paulo: Saraiva, 2007.

CASTRO, Domingos Poubel. **Auditoria e Controle Interno na Administração Pública**. Ed. 2. São Paulo: Atlas, 2009.

COIMBRA, Fábio. **Estruturação de unidade de gestão de riscos operacionais em bancos: um estudo de caso**. Dissertação para Tese de Mestrado, Universidade de São Paulo, São Paulo, SP, 2006. Disponível em: <http://www.teses.usp.br/teses/disponiveis/12/12139/tde-23042007-164724/pt-br.php> acesso em: 11 jan. 2014.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Resolução 750, de 29 de dezembro de 1993: Princípios de Contabilidade (PC). (Redação dada pela Resolução CFC nº. 1.282/10)**. Brasília DF: CFC, 1993. Disponível em: <http://www.cfc.org.br/sisweb/sre/docs/RES_750.doc>. Acesso em: 22 fev. 2014.

_____. **Resolução 1.230, de 04 de dezembro de 2009: NBC TA 610; utilização do trabalho de especialistas**. Brasília DF: CFC, 2009. Disponível em <http://www.cfc.org.br/uparq/NBCTA610.pdf>. Acesso em: 22 fev. 2014.

_____. **Resolução 920, de 09 de janeiro de 2002: NBCT 10.8; entidades cooperativas**. Brasília DF: CFC, 2002.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY. COMMISSION (COSO). **Gerenciamento de riscos corporativos: estrutura integrada**. Jersey City: COSO, 2007. Disponível em <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em: 22 mar. 2014.

CROUHY, Michel; GALAI, Dan; MARK, Robert. **Fundamentos da gestão de Risco**. 1. ed. São Paulo: Serasa, 2007.

DIONNE, Georges. RISK MANAGEMENT: HISTORY, DEFINITION, AND CRITIQUE. Risk Management and Insurance Review, v.16, n. 2, p.147-166, 2013

ELO GROUP. **Boas Práticas para o Uso Estratégico de Controles Internos**. Rio de Janeiro: ELO Group, 2007. Disponível em: <http://www.bpmglobaltrends.com.br/wp-content/uploads/2014/01/4-Boas_praticas_para_o_uso_estrategico_de_controles_internos.pdf>. Acesso em 22 fev. 2014.

HORI, André Shirengu. **Modelo de gestão de risco em segurança da Informação: um estudo de caso no mercado brasileiro de Cartões de Crédito**. Dissertação de Mestrado – FGV, São Paulo, 2003. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2216/74539.pdf?sequence=2>. Acesso em: 04 mar. 2014.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 6 ed. São Paulo: Atlas, 2007.

LANCELOTTI, Mário Luiz. **Redes de Autoatendimento Bancário no Brasil – Estudo do Compartilhamento**. Dissertação de Mestrado, Centro Universitário Nove de Julho – UNINOVE, São Paulo, 2005.

MACHADO, Rosane. **Análise da relação entre a gestão de riscos da tecnologia da informação (TI) e a gestão de riscos corporativos**. Tese de Mestrado, Universidade do Vale do Rio dos Sinos. São Leopoldo, 2012.

MARSHALL, Cristopher. **Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras**. Ed. Especial para Ademar Shardong. Rio de Janeiro: Qualitymark, 2002.

PEDOTE, C. **Análise e Gerenciamento de Risco: Gestão do Risco Operacional em Instituições Financeiras**. Dissertação (Mestrado em Administração). Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas. 2002. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/4919/1200200870.pdf?sequence=1>. Acesso em: 04 mar. 2014.

PORTER, M. **Competição: Estratégias Competitivas Essenciais**. Brasilia, Brazil: Campus, 1990.

RICHARDSON, Roberto Jarry et al. (Colaboradores). **Pesquisa social: métodos e técnicas**. 3 ed. São Paulo: Atlas, 2008.

RODRIGUES, Maicon Antonio. **Padronização e controles internos do produto cartão Sicredi: aplicados à conciliação contábil das transações com cartão funcionalidades débito e crédito**. TCC. Faculdade Porto-alegrense – FAPA. Porto Alegre, 2012.

SAUNDERS, Anthony. **Administração de Instituições Financeiras**. Ed. 2. São Paulo: Atlas, 2007.

SOUZA, Sandra Regina Silva dos Santos. **Mudanças com a introdução da "Automatic Teller Machine": um estudo de caso num grande banco nacional**. Dissertação de Mestrado, Fundação Escola de Comercio Álvares Penteado. São Paulo, 2001.

TECBAN. **Tecnologia Bancária**. Disponível em <www.tecban.com.br>. Acesso em: 22 mar. 2014.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. 4 ed. Bookman, Porto Alegre, 2010.