Gestão de risco operacional: um estudo de caso da capacidade de resposta a incidentes operacionais em empresas financeiras

Operational risk management: a case study of the ability to respond to operational incidents in financial companies

Recebido: 20/01/2020 – Aprovado: 10/04/2020 – Publicado: 01/05/2020

Processo de Avaliação: Double Blind Review

Rolf Henrique Neubarth[1]

Mestre em Governança Corporativa FMU – Centro Universitário das Faculdades Metropolitanas Unidas (FMU)

Alessandro Marco Rosini[2]

Pós-Doutor em Administração de Empresas pela Universidade de São Paulo (FEAUSP)

Professor da Universidade Anhanguera (UNIAN/SP) e do Centro Universitário da Várzea Grande (UNIVAG/MT)

Renata Carolina Grotta[3]

Mestre em Governança Corporativa FMU – Centro Universitário das Faculdades Metropolitanas Unidas (FMU)

Eduardo Ribeiro Guedes[4]

Mestre em Governança Corporativa FMU – Centro Universitário das Faculdades Metropolitanas Unidas (FMU)

RESUMO

A gestão de risco tem papel importante como parte da governança corporativa das empresas da indústria financeira. Assim, este artigo tem como objetivo analisar a capacidade que as empresas da indústria financeira possuem em responder a um evento de crise total de interrupção em seus *sites* principais de operação. Para isso, foi realizado um estudo qualitativo com análise de múltiplos casos, em quatro instituições financeiras nacionais e estrangeiras, que operam no sistema financeiro brasileiro. Os resultados obtidos demonstram que as instituições financeiras de grande porte, que em geral são os bancos múltiplos de varejo, investem fortemente em governança corporativa e

[1] Autor para correspondência: Centro Universitário das Faculdades Metropolitanas Unidas- Av. da Liberdade, 899 - Liberdade, São Paulo - SP, 01503-001. Brasil. E-mail: henrique.fgvti@gmail.com

[2] E-mail: alessandro.rossini@yahoo.com

[3] E-mail: renata_grotta@yahoo.com.br

[4] E-mail: erguedes@gmail.com

segurança da informação, como também em implementar políticas de gestão de risco operacional, infraestrutura redundante e testes que validem se este investimento trará, de fato, uma resposta a qualquer evento de crise.

Palavras-chave: Gestão de Risco; Recuperação de Desastres; Gestão de Continuidade de Negócios; Governança Corporativa.

ABSTRACT

Risk management has an important role as part of the corporate governance of companies in the financial industry. Thus, this article aims to analyze the ability of firms in the financial industry have to answer a total crisis interruption event in its main sites of operation. For this, was held a qualitative multiple case studies in four national and foreign financial institutions operating in the Brazilian financial system. The results show that large financial institutions, which are usually multiple retail banks, invest heavily in corporate governance and information security, as also to implement operational risk management policies, redundant infrastructure and testing to validate if this investment will, in fact, to respond to any crisis event.

Keywords: *Risk Management; Disaster Recovery; Business Continuity Management; Corporate Governance.*

1. INTRODUÇÃO

As instituições financeiras estão sempre lidando com análises de riscos e com a possibilidade de perdas potenciais em suas operações. Com os modelos de negócios globalizados e a necessidade crescente de aumentar a eficiência operacional associada aos controles em suas operações, as instituições financeiras demandam por maior adoção de práticas de gestão de risco operacional e continuidade de negócios, que possibilitem as organizações uma resposta eficiente, em caso de qualquer evento não esperado, e que coloque em risco a continuidade de suas operações.

Sendo assim, a gestão de risco operacional pode possibilitar a identificação dos principais processos críticos das instituições financeiras, que devem ser recuperados ou blindados, para que possibilitem o foco dos seus investimentos (*RMA*, 2015).

Na identificação dos principais processos da gestão de risco operacional, devem ser consideradas quais as plataformas, quais os potenciais pontos de falhas, quem são os *key-players* para continuar suas liquidações financeiras, quais são os impactos de negócios, quais são os métodos alternativos de realizar suas operações e quais são os principais fornecedores. A identificação desses processos permite entender como minimizar a probabilidade de ter perdas derivadas de desastres e crises operacionais, como executar um plano de resposta e comunicação para clientes, *stakeholders*, reguladores e mercado, de forma estruturada e provendo ferramentas para ações em momentos de crise (*RMA*, 2015; Hoffman, 2002; Shea, 2006).

Nos mapas de gestão de riscos existentes nas instituições financeiras brasileiras, baseados no Conselho Monetário Nacional – CMN (2015) e no Banco Central do Brasil – Bacen (2015), quanto à adequação aos princípios de Basileia III Pilar 3, existem os seguintes tipos de riscos com os quais as instituições financeiras, autorizadas a funcionar pelo Bacen e as administradoras do consórcio, devem considerar os riscos de mercado, de liquidez, de crédito e operacional.

A gestão do risco pode ser definida como um conjunto de processos que proporcione a identificação e implementação de medidas de proteção, para a diminuição dos riscos que podem ocorrer com os ativos de informação das organizações, e harmonizá-los com os custos operacionais e financeiros abrangidos (Beal, 2005).

A gestão de risco e continuidade de negócios possui grande importância para as empresas, negócios e até mesmo para os governos. Isso se dá porque, em um mundo que se conecta e opera 24 horas por dia, sete dias por semana e 365 dias no ano, não é possível parar ou operar sem um plano de resposta a incidentes ou eventos, uma vez que tais incidentes e eventos podem impactar as plataformas, sistemas, mercados e interesses das organizações. Para alcançar seus objetivos organizacionais, as organizações devem manter-se disponíveis e buscar incessantemente um alto grau de resiliência aos negócios.

Sendo assim, alavancados pelo atentado do 11 de Setembro, aquele que talvez tenha sido um dos mais significativos eventos de crise para a indústria financeira observado até o momento, verifica-se um grau elevado de investimento em gestão de risco, governança corporativa e gestão de segurança da informação. Esses investimentos visam garantir o retorno e resultados esperados pelos acionistas, com apoio aos sistemas das empresas.

Nesse contexto, este artigo tem como objetivo analisar a capacidade que as empresas da indústria financeira possuem em responder a um evento de crise total de interrupção em seus sites principais de operação.

A metodologia utilizada diz respeito a uma análise qualitativa, utilizando múltiplos casos, em quatro instituições financeiras nacionais e estrangeiras, que operam no sistema financeiro brasileiro, em diferentes tamanhos e operações.

2. REFERENCIAL TEÓRICO

A gestão de risco operacional e continuidade de negócios pode ser claramente associada às disciplinas de segurança da informação ou mesmo de gestão operacional (Monks & Minow, 1995). Isso ocorre porque as ações para estabelecer um modelo de governança de segurança da informação são praticamente os mesmos que devem ser seguidos quando se trata de criar um modelo de governança de gestão de risco operacional e continuidade de negócios, uma vez que em seu cerne, ambas identificam os principais riscos que uma organização pode estar suscetível, como, por exemplo, ter suas operações paralisadas, suas liquidações financeiras interrompidas ou mesmo riscos de imagem em jogo.

É importante ressaltar a intrínseca e inseparável relação que a gestão de segurança da informação possui com a gestão de risco e continuidade de negócios, pela necessidade de disponibilização da informação (Monks & Minow, 1995).

Portanto, é desejável que as políticas de governança corporativas, gestão de segurança de informação e continuidade de negócios estejam alinhadas e em sincronia para que possam trazer efetividade aos organismos aos quais estão associadas.

De acordo com Monks e Minow (1995), a governança corporativa trata de um conjunto de leis e regulamentos que visam:

- Garantir os direitos dos acionistas das empresas, controladores ou minoritários;
- Disponibilizar informações, de forma que os acionistas acompanhem as decisões que impactam negócios e avalie o quanto elas interferem em seus direitos;
- Possibilitar aos diferentes acionistas e diferentes públicos (*stakeholders*), alcançados pelos atos das empresas, tenham instrumentos que possam assegurar a observância dos seus direitos;
- Todos os itens citados acima também permeiam a gestão de risco e continuidade de negócios, bem como a gestão de segurança da informação, criando assim um sincronismo entre as três disciplinas supracitadas (Monks & Minow, 1995).

Portanto, a identificação, avaliação e busca da resiliência aos riscos da organização, com a busca do equilíbrio das equações de custos e investimentos, é um dos resultados esperados quando se tem essas três disciplinas integradas.

A informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo. Portanto, a informação deve ser mantida de forma a estar sempre protegida de ameaças a sua integridade e confidencialidade, seguro e disponível para o acesso (Beal, 2005). Inclusive de acessos não autorizados, alterações indevidas, ou com as interrupções não previstas, ou seja, não intencionais, que configuram quebra de disponibilidade (Sêmola, 2003).

As boas práticas podem ser definidas como métodos ou programas que foram identificados como bem-sucedidos em alcançar seus objetivos em suas respectivas disciplinas, que podem ser usadas, adaptadas ou adotadas parcialmente, para atuar nas circunstâncias a que se propõem dentro dos sistemas das empresas.

Atualmente, para a gestão de risco e continuidade de negócios, conta-se com dois grandes institutos que criaram *frameworks* que proveem as melhores práticas de GCN – Gestão de Continuidade de Negócio, para o meio corporativo. São eles:

- *Disaster Recovery International Institute* – DRII: é uma entidade sem fins lucrativos responsável por pesquisar a governança de gestão de risco e continuidade de negócios com oferta de certificações. É um *framework* de boas práticas de atuação na disciplina desde 1988 e possui mais de 10.000 profissionais certificados, de várias indústrias, negócios e setores de mercados distintos, ao redor do mundo. A certificação emitida sob avaliação aplicada pelo instituto garante que os profissionais tenham a proficiência necessária para atuar em nível sênior na gestão de risco e continuidade de negócios.
- *Business Continuity Institute* – BCI: estabelecido em 1994 como uma entidade que busca promover as boas práticas de governança, na disciplina de gestão de risco e continuidade de negócios, com alta maturidade, e que fortaleça o nível de resiliência de comunidades, sejam elas governamentais ou privadas. O BCI se posiciona como uma entidade que preza pela excelência em continuidade de negócios, e suas certificações proveem validação técnica e profissional para gestão de risco e continuidade de negócios.

3. METODOLOGIA

Para compreender a capacidade de resposta aos eventos, avaliando se os modelos de gestão de risco e continuidade de negócios são validados e testados, optou-se por um estudo de caso. Segundo Yin (2006), a escolha de projeto de caso único ou múltiplo depende do plano de pesquisa ao qual o pesquisador tem por princípio investigar. Como o objetivo é avaliar a gestão de riscos e continuidade de negócios em um segmento específico, esta pesquisa utiliza múltiplos casos, incluindo empresas nacionais e multinacionais indicadas para representar o fenômeno no universo das instituições financeiras no Brasil.

Para a realização da pesquisa, foram selecionadas quatro empresas de perfis e portes diferentes, com operações distintas, mas que seguem a regulamentação do Bacen (Resolução n. 3.380) ou CMN (2015). A diversificação foi fundamental para a

ampliação da visão do tratamento do risco operacional, principalmente em um mercado regulado. Dentre as empresas selecionadas, três são bancos e uma é corretora de valores.

Por ser um assunto que pode expor as instituições analisadas, o nome das empresas será preservado. A pesquisa vai tratar cada instituição por uma letra do alfabeto. A instituição A é um banco multinacional com capital de origem estrangeira com sede em Nova York, Estados Unidos, com escritório em São Paulo, e está presente em 160 países no mundo. A instituição B é um banco multinacional de capital estrangeiro com sede em Nova York, Estados Unidos, que não possui operação de varejo no Brasil e opera somente no mercado corporativo financeiro com uma crítica operação de *trade*. A terceira instituição, chamada de instituição C, é um banco de capital público de grande porte, com forte atuação no varejo, presença em território nacional, e sede em Brasília. A instituição D é uma corretora de valores de menor porte, com atuação nacional, mas operação centralizada em São Paulo.

Dessa forma, a Tabela 1 apresenta os dados resumidos das quatro empresas da indústria financeira investigadas, que atuam no mercado financeiro brasileiro, sendo três no segmento bancário e uma no segmento de corretagem de valores.

Tabela 1 – Resumo das características de cada instituição pesquisada.

Instituição	A	B	C	D
Gênero	Financeiro	Financeiro	Financeiro	Financeiro
Principal Setor	Banco	Banco	Banco	Corretora de Valores
Posicionamento	Múltiplo (Var. e Corp.)	Corporativo Investimento	Múltiplo (Var. e Corp.)	Corretora de Valores
Capital	Privado/Estrangeiro	Privado/Estrangeiro	Público/Nacional	Privado/Nacional
Funcionários	5.000	600	96.800	50
Agências	86	N/A	4.000	N/A
Net Income 2014	R$ 2,3 Bilhões	Não Divulgado	R$ 6,1 Bilhões	Não Divulgado
Site Operação Principal	3	1	3	1
Site Operação Alternativo	1	1	2	0

Fonte: dados coletados nas entrevistas realizadas nas instituições, em setembro 2015.

Em se tratando de uma pesquisa qualitativa, serão utilizados procedimentos etnográficos, visando à compreensão da visão humana, principalmente aquela

relacionada com os gestores que cuidam das políticas e demais aspectos dos planos de recuperação de desastres. A opção por entrevistar diretamente gestores foi a melhor forma de avaliar aspectos intrínsecos na continuidade de negócios. Aspectos estes que dificilmente seriam passíveis de avaliação apenas em análise de documentos ou mesmo dos números relacionados com os testes de recuperação de desastres.

Para cada instituição pesquisada, as entrevistas foram estruturadas em três grandes tópicos: gestão de risco operacional, local (*site*) alternativo e infraestrutura de contingência, governança de TI e segurança da informação em apoio à disciplina de risco. Para avaliar o grau de resiliência, os principais pontos do levantamento são:

- Ferramentas que a organização possui para reagir a um evento de total indisponibilidade;
- Tempo de resposta dos testes em relação à necessidade do negócio;
- Boas práticas de governança corporativa e governança de TI que suportem a resposta a um evento de crise;
- Critérios de sucesso e validação dos testes de recuperação de desastres.

As entrevistas com os gestores de continuidade de negócio, quando existentes nas empresas pesquisadas, ou de gestores de tecnologia da informação, quando estes forem os responsáveis pelo tema, foram conduzidas dando visibilidade ao que foi considerado conceito de classificação de boa prática de validação dos planos de recuperação. As entrevistas buscam encontrar evidências sobre como as áreas de negócio das empresas validaram as manobras e os procedimentos de recuperação baseadas na avaliação dos seus processos críticos. Além disso, as entrevistas visam explorar como os gestores de risco operacional ou de tecnologia da informação executam o pós-teste, documentando todo o processo.

Ainda dentro do processo de coleta, buscou-se identificar o perfil dos profissionais participantes, como sua formação, sua experiência em gestão de risco e continuidade de negócios, formação acadêmica, e se possuía alguma certificação em gestão de risco e continuidade de negócios. Ainda foi verificado se as empresas utilizam procedimentos de gestão de risco e continuidade de negócios associados a alguma boa prática adotada no mercado nacional ou internacional. Na terceira fase da entrevista, buscou-se avaliar o nível de maturidade empregado especificamente no aspecto relacionado em testar e

validar os planos de contingência estruturados, com objetivo de identificar se estes são testados considerando uma indisponibilidade total das operações.

4. ANÁLISE E DISCUSSÃO DOS DADOS

As instituições foram pesquisadas considerando os testes realizados pelas mesmas, baseados na entidade *Disaster Recovery International Institute* – DRII, que estão descritos na Tabela 2.

Tabela 2 – Descrição dos testes realizados.

	Tolerância a Falha (*Failover Strategy*)	**Cenário de Total Indisponibilidade** (*Worst Case Scenario*)
Teste de Mesa (*Tabletop*)	Usado como teste tático. Pode ser usado para ambas as situações. Trata-se de organização de ações, planejamento e validações para que o tático dos planos de recuperação esteja alinhado com a estratégia de continuidade de negócios	
Teste de Componente	Usado para validar que um determinado componente seja recuperado em caso de interrupção	Não aplicável
Teste de Plataforma	Usado para determinar um conjunto de componentes que componham uma plataforma seja testado	Parcialmente aplicável
Teste Operacional	Aplicável somente para conectividades (roteadores de borda ou DMZs)	Usado para simular a perda total do ambiente produtivo envolvendo todos os times críticos da organização

Fonte: *Disaster Recovery International Institute* – DRII.

A entrevista com a instituição A foi realizada na própria empresa diretamente com o gestor de continuidade de negócios.

- **Governança de Risco Operacional:** a área de gestão de continuidade de negócios possui 04 funcionários dedicados para atuar na governança de continuidade de negócios, sendo que todos possuem treinamento e certificação na disciplina de gestão de continuidade de negócios. A instituição possui uma política de continuidade de negócios implementada, que garante que todos os

níveis críticos da empresa participem e se engajem no desenvolvimento de estruturados planos de recuperação de desastres. A empresa possui um calendário de testes incluindo testes de indisponibilidade total do *site* de operações principal. Nessa manobra, as áreas de negócio participam e validam que a manobra de testes foi ou não realizada de forma bem-sucedida, com coletas de evidências de telas de sistemas e lançamentos em bases que são descartadas ao final do teste. Os Objetivos de Tempo de Recuperação (RTO – *Recovery Time Objetive*) são medidos e as diligências de lições aprendidas são realizadas com cada área participante. O RTO – *Recovery Time Objetive* é o tempo necessário para que um plano de contingência seja ativado após a declaração da contingência.

- ***Site* Alternativo e infraestrutura de contingência:** a instituição bancária A possui um *site* próprio alternativo, com posições de trabalho alternativas, e com toda a infraestrutura de TI e tecnologia de replicação de dados críticos implementados, com espelhamento *hot swap* de servidores, plataformas, base de dados e telecomunicações replicadas, com abordagem dupla, com roteadores e operadoras de serviço de dados diferentes para garantir alta disponibilidade de acesso de tráfego de dados com as agências, mercado financeiro e instituições B2B, em caso de queda de um dos *links*.

- **Governança de TI e Segurança da Informação em apoio à disciplina de risco operacional:** a instituição A possui governança de TI baseada nas boas práticas do *framework* do ITIL, possibilitando a verificação de que a gestão de mudanças é forte e atuante na empresa, com processos bem definidos e sendo seguidos pelas áreas de desenvolvimento e infraestrutura da organização. Isso garante que todas as atualizações de sistemas e versões estejam sendo atualizadas, tanto no *site* principal como no *site* de contingência. Já na gestão de problemas e incidentes, esta se apoia na identificação de SPOFs (*single point of failure*), que é um processo que garante o mapeamento da estrutura, evitando pontos que não estejam devidamente projetados em contingenciamento de infraestrutura e de impactos grandes na operação. No caso da instituição A, a empresa vem atuando com controles internos de *Risk Control Self Assessment*, apoiado pela interseção com a disciplina de segurança da informação.

Essa estrutura de *site* alternativo da instituição A, aliada ao seu grau de governança de TI, e sua política de continuidade de negócios e segurança da informação, que atua em praticamente todos os níveis da empresa, possibilitam que o time de gestão de risco operacional desenvolva uma manobra de testes que possa validar fim a fim um teste. Isso garante que a instituição conseguirá responder a um evento de crise de grandes proporções dentro do prazo esperado pelos acionistas, alcançando o RTO – *Recovery Time Objetive.*

A entrevista com a instituição B foi realizada por telefone com o gestor de continuidade de negócios. O resumo da entrevista e os resultados da análise estão apresentados nos tópicos abaixo:

- **Governança de Risco Operacional**: além do gestor de risco operacional, a área possui mais dois funcionários dedicados a esta disciplina, somando um total de 03 funcionários dedicados para a gestão de continuidade de negócios. Mesmo com uma operação menor em termos de volume e processamento, o modelo de continuidade de negócios da instituição B é bem similar ao da instituição A. Todos também possuem treinamento e certificação na disciplina de gestão de continuidade de negócios. Nos testes, as áreas de negócio participam, mas não efetuam lançamentos operacionais nos sistemas, apenas concretizam o acesso aos sistemas disponíveis no teste. Ou seja, não há garantia que os sistemas funcionem em um cenário de contingência.
- ***Site* Alternativo e infraestrutura de contingência:** A instituição bancária B possui um *site* alternativo, com posições de trabalho alternativas, infraestrutura de TI e tecnologia de replicação de dados críticos, espelhamento de servidores, plataformas, base de dados e telecomunicações replicadas em situação de balanceamento de carga de tráfego de dados, ou seja, pode garantir que o tráfego de dados seja feito a partir de ambas as conexões ao mesmo tempo, com abordagem dupla, com roteadores e operadoras de serviço de dados diferentes, para garantir alta disponibilidade de acesso de tráfego de dados, em um *site* contratado no mercado. Essa instituição não possui agências. Seu *core business* é focado em operações de *trade*, derivativos, FX, cofre, custódia e produtos bancários corporativos. A instituição B possui conectividade com o mercado financeiro e instituições B2B. Porém, toda a infraestrutura alternativa não é ativo da empresa.

- **Governança de TI e Segurança da Informação em apoio à disciplina de risco operacional:** a instituição B possui uma governança de TI bem estruturada. Possui interseções com as disciplinas de gestão de problemas e incidentes e gestão de mudanças. Como as plataformas no *site* alternativo são geridas pela própria TI da instituição, o fato do ambiente estar em um *datacenter* alugado não impede que as versões dos ambientes na estrutura de produção estejam em sincronia com a estrutura de contingência. Há um forte controle nos processos de análise de fornecedores para garantir que, contratualmente, a opção por um *site* alternativo não crie nenhuma questão de segurança para a empresa. O contrato possui cláusulas pesadas de confidencialidade.

A estrutura de *site* alternativo da instituição B possui apenas um ponto a ser considerado, uma vez que ela possui espaço compartilhado com outras empresas que porventura também possam ter o mesmo modelo de contrato com outros clientes. Nesse ponto, pode ser observada a primeira evidência de gerenciamento de risco *versus* o investimento de ter um *site* dedicado.

A empresa B possui alto grau de governança de TI e também uma política de continuidade de negócios e segurança da informação, que atuam em todos os níveis da empresa, possibilitando que o time de gestão de risco operacional desenvolva uma manobra de testes que valide toda a cadeia de produção crítica. Isso garante que a instituição conseguirá responder a um evento de crise de grandes proporções, dentro do prazo esperado pelos acionistas, alcançando também o RTO – *Recovery Time Objetive*, que significa Objetivo de Tempo de Recuperação.

A instituição C é uma grande instituição com alcance nacional no segmento bancário do varejo. Tal instituição possui várias áreas em prédios distintos, descentralizando sua operação crítica, tanto de áreas de negócio como de tecnologia da informação, possibilitando a opção de mais cenários de estratégia de recuperação. A entrevista com a instituição C também foi realizada por telefone com o gestor de continuidade de negócios, com o resumo e os resultados apresentados nos tópicos a seguir:

- **Governança de Risco Operacional**: além do gestor de continuidade de negócios, a área possui mais oito funcionários dedicados a esta disciplina, somando um total de 09 funcionários, que atuam não só para a gestão de continuidade de negócios, mas também para apoiar em processos de segurança

da informação, quando realizam processos de análise de segurança de perímetro e segurança do trabalho, com atuação em processos com a CIPA, por exemplo. Esses profissionais interagem com a área de TI, e, também, executam a revisão de processos de negócios junto às áreas críticas. O modelo de governança de continuidade de negócios da instituição C é semelhante aos das instituições A e B, com alto grau de maturidade nas revisões de processos e análise de impacto ao negócio.

- ***Site* Alternativo e infraestrutura de contingência:** a instituição bancária C possui *site* alternativo com posições de trabalho alternativas, com toda a infraestrutura de TI e tecnologia de replicação de dados críticos para o seu principal *site*, que abriga o *datacenter* e as áreas de negócios com *core business* na operação de varejo. Ela também possui espelhamento de servidores e plataformas, base de dados e telecomunicações replicadas, com abordagem dupla, com roteadores e operadoras de serviço de dados diferentes, para garantir alta disponibilidade de acesso de tráfego de dados. A instituição C executa testes cíclicos com dimensão de testes operacionais, considerando um cenário de total interrupção, mas possui estratégias diferenciadas, pois possui um porte maior com 03 *datacenters*, que trabalham em modo clusterizado de replicação de dados. O processo de clusterização se dá por meio de mais de um componente de infraestrutura, que atuam de forma simultânea, fazendo com que esses componentes sejam percebidos pelo resto dos ambientes tecnológicos de forma única.

- **Governança de TI e Segurança da Informação em apoio à disciplina de risco operacional:** por ser um banco com uma larga operação nacional de varejo, a empresa possui grandes dimensões, e quando se há grandes operações para serem geridas, as empresas precisam estar alinhadas a boas práticas de gestão. A gestão de problemas e incidentes e a gestão de mudanças ocorrem para ambientes de *mainframe* e plataforma média, garantindo que os *sites* de contingência e produção estejam nas mesmas versões.

  Esta estrutura de *site* alternativo da instituição C também confere a esta instituição, um alto grau de resiliência em caso de um evento que impacte sua operação. Ela possui *sites* alternativos, tanto para pessoas como para a replicação de suas principais plataformas de tecnologia. A empresa C também

possui um alto grau de governança de TI, assim como possui uma política estruturada de continuidade de negócios e segurança da informação, que atua em praticamente todos os níveis da empresa, possibilitando que o time de continuidade de negócios desenvolva uma manobra de testes que possam ser validados, e que garantam que a instituição possa responder a um evento de crise de grandes proporções dentro do prazo esperado, alcançando o RTO – *Recovery Time Objetive*.

- **Governança de Risco Operacional**: esta instituição não possui profissionais dedicados de gestão de continuidade de negócios. Há um auditor que documenta as regulamentações necessárias em todas as disciplinas incluindo a gestão de risco operacional. Esse auditor atua em conjunto com o gestor de tecnologia da informação, que possuem a responsabilidade de garantir que a infraestrutura de acesso aos sistemas de *trader*, que são as plataformas relacionadas ao negócio da instituição mencionada. Estas plataformas disponibilizam os *softwares* utilitários, com informações integradas sobre fundos de investimentos, mercado da Bolsa da Valores de São Paulo – BM&FBOVESPA, operações financeiras de forma eletrônica, informações de mercado especializadas, carteira de clientes e todas as informações necessárias que sejam pertinentes aos negócios da empresa.

- ***Site* Alternativo e infraestrutura de contingência:** a instituição D não possui um *site* alternativo com posições de trabalho para o caso de uma indisponibilidade completa. Apenas sua infraestrutura de TI é contingenciada em um *datacenter* contratado onde existe um contrato de utilização de máquinas servidoras. Sua recuperação de dados e plataformas de suporte ao negócio é realizada por meio da restauração de *backup*, a partir de mídias que se encontram no mesmo *site* de contingência que é contratado no mercado. O contrato também prevê a utilização de armazenagem de mídias em um ambiente controlado e climatizado. Essa empresa não possui tecnologia de replicação de dados críticos ou espelhamento de servidores, plataformas, base de dados e telecomunicações.

- **Governança de TI e Segurança da Informação em apoio à disciplina de risco operacional:** a instituição D não possui um processo de gestão de TI devido ao seu universo tecnológico ser de pequeno porte. Dessa forma, todos os

sistemas críticos são contingenciados por meio de *backup* incremental realizado diariamente. Sua demanda de atualização de bases de problemas e controle de mudança é muito pequena, apesar de existente, mas sua escala é menor. Sua demanda por uma disponibilidade é limitada ao período em que o sistema financeiro opera sem demandas de maiores demandas de disponibilidade em finais de semana ou fora do horário de operação financeira, e isso os torna enxutos para esses controles.

A tabela 3 apresenta os resultados resumidos das entrevistas realizadas, encontrados nas quatro instituições pesquisadas.

Tabela 3 – Resumo dos resultados encontrados nas quatro instituições pesquisadas.

nstituição	**A**	**B**	**C**	**D**
Possui políticas ou diretriz de GCN	Sim	Sim	Sim	Sim
Planos e análise de impacto do negócio estão documentados	Sim	Sim	Sim	Sim
Os Objetivos de Tempo de Recuperação (RTO) são alcançados nos testes de acordo com o que é refletido no BIA (*business impact analysis*)	Sim	Sim	Sim	Não é validado
Os *stakeholders* participam e formalizam a participação nos testes provendo o *sign-off* que os testes de contingência foram consistentes de acordo com o que foi planejado	Sim	Sim	Sim	Não
Há revisões de lições aprendidas e ações de análise de pós-teste?	Sim	Sim	Sim	Não

Fonte: Dados da pesquisa.

Nas entrevistas realizadas nas quatro instituições que operam na indústria financeira brasileira, foi avaliado o grau de maturidade de resiliência em cada instituição, em caso de um evento de crise ou incidente de grandes proporções em seus sites principais de operação.

Das quatro empresas avaliadas, três possuem alto investimento e alto grau de maturidade na gestão de risco operacional (instituições A, B e C). A quarta instituição de porte menor – instituição D, possui uma gestão de risco operacional que lhe confere respostas a determinados incidentes de proporções menores, que caso venham a existir, serão respondidos como uma forma de tolerância à falha. Porém, isso não significa que,

em uma situação de um evento crítico de grandes proporções, a instituição D não terá seu tempo de resposta dentro da expectativa de seus acionistas.

Pode-se verificar também que, nos bancos de varejo, as operações possuem um grau de resiliência maior, em comparação com instituições que não operam nesse segmento de negócios. Tais organizações investem fortemente não apenas em governança corporativa e segurança da informação, mas também em implementar políticas de gestão de risco operacional, infraestrutura redundante e testes que validem se esse investimento trará, de fato, uma resposta a qualquer evento de crise de grandes proporções. Para as instituições que não possuem demanda de disponibilidade de 24 horas por dia em operações *on-line*, é requerido um investimento menor em *sites* alternativos, replicações de ambiente tecnológico e redundância de sistemas críticos.

5. CONSIDERAÇÕES FINAIS

Os riscos operacionais podem ser definidos como as perdas potenciais resultantes de gestão de sistemas inadequados, ou mesmo de uma administração que não seja adequada (Jorion, 1997). E, segundo Monks e Minow (1995), a gestão de risco operacional e continuidade de negócios pode ser claramente associada às disciplinas de segurança da informação ou mesmo de gestão operacional. Dessa forma, a gestão de risco e continuidade de negócios tem papel importante como parte da governança corporativa das empresas da indústria financeira. Nesse sentido, as empresas dessa indústria possuem estruturações de tecnologia, processos bem documentados, recursos investidos em redundância de *sites*, redundância de plataformas de tecnologia e engajamento das áreas de negócio.

Os investimentos em gestão de risco e continuidade de negócios das empresas da indústria financeira são importantes, uma vez que, de acordo com Silva (2006), a governança corporativa é um processo em que as empresas precisam atrair capital externo, e com isso, a necessidade de se mostrarem organizadas, transparentes e preparadas para um ganho de escala em que continuem mantendo seus controles, sua gestão, transparência e sua resiliência.

Nesse sentido, pode-se verificar que, as instituições financeiras de grande porte, que em geral são os bancos de varejo múltiplos, e, portanto, operam em regime de 24 horas por

dia e 7 dias por semana, com operações de liquidação financeira, operações de cartões de crédito que geram operações 24 horas, e com transações críticas de mercado em termos de volume e quantidade de liquidação financeira envolvidas, que podem comprometer o mercado financeiro devido ao risco sistêmico de impacto financeiro, estas empresas investem fortemente não só em governança corporativa e segurança da informação, mas também em implementar políticas de gestão de risco operacional, infraestrutura redundante e em testes que validem se este investimento trará de fato uma resposta a qualquer evento de crise de grandes proporções, que indisponibilize suas operações em seus *sites* principais.

O estudo também verificou que é requerido um investimento, para as instituições que não possuem demanda de disponibilidade de 24 horas por dia em operações *on-line*. Outro aspecto relevante do estudo é a análise de investimento *versus* o apetite ao risco. As empresas B e D não tinham *sites* dedicados associados à análise dos riscos, e concluíram que um investimento em um *site* dedicado não se justifica, uma vez que eles não possuem a necessidade de responder com um RTO agressivo, podendo executar manobras de contingência junto ao Banco Central Brasileiro, até que se consiga reestabelecer as operações mais críticas. Isso se dá porque as instituições que investem em *sites* alternativos dedicados são os bancos com modelos de produtos múltiplos com operações no varejo.

Embora o estudo tenha demonstrado que nenhum dos bancos múltiplos tenha somente testes de operação sendo feitos, a pesquisa mostrou que eles possuem um foco grande nesse tipo de teste, considerando o pior cenário, pois, com isso, é possível testar a interação dos times de tecnologia e dos times críticos de operações do negócio, das plataformas e das entradas e saídas (*input e output*) de processos.

Pode-se concluir também que existe um grande distanciamento dos bancos múltiplos de varejo com relação aos investimentos em governança de TI e gestão de risco operacional, que obtiveram alto desempenho em relação às demais instituições pesquisadas. Nesse sentido, estes poderiam constituir-se em *benchmarks* para os demais bancos múltiplos que queiram avaliar sua governança de gestão de risco operacional e continuidade de negócios, e, com isso, fortalecer sua avaliação de resiliência.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002:2005 – *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação*. Rio de Janeiro: ABNT.

ASSI, Marcos. (2012). *Gestão de riscos com controles internos: ferramentas, certificações e métodos para garantir a eficiência dos negócios*. São Paulo: Ed. Sant Paul Editora.

Banco Central do Brasil. Recuperado em 26 setembro, 2015, de http://www.bcb.gov.br/pt-br

BEAL, A. (2005). *Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação das organizações*. São Paulo: Ed. Atlas.

Bertucci, J. L. de O. (2008). *Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC): ênfase na elaboração de TCC de pós-graduação lato sensu*. São Paulo: Ed. Atlas.

BCI – Business Continuity Institute. Recuperado em 26 setembro, 2015, de http://www.thebci.org/.

Brito, O. (2010). *Gestão de riscos: Uma abordagem orientada a riscos operacionais*. São Paulo: Ed. Saraiva.

Campos, A. (2007). *Sistemas de segurança da informação* (2ª ed.). Florianópolis: Ed. Visual Books.

CMN – Conselho Monetário Nacional. Recuperado em 26 setembro, 2015, de https://www.bcb.gov.br/?CMN

Da Silva, E. C. (2006). *Governança corporativa nas empresas: guia prático para acionistas e conselho de administração. Novo modelo de gestão para redução do custo de capital e geração de valor ao negócio*. São Paulo: Ed. Atlas.

DRII – Disaster Recovery International Institute. Recuperado em 26 setembro, 2015, de https://www.drii.org/

Guindani, A. (2011). *Deus é Brasileiro: O guia da gestão de continuidade de negócios.* Rio de Janeiro: Ed. Ciência Moderna.

Hoffman, D. G. (2002). *Managing operational risk: 20 firmwide best practice strategies*. New York: Ed. John Wiley & Sons.

Jorion, P. (1997). *Value at risk: the new benchmark for controlling market risk*. New York: Ed. McGraw-Hill.

Monks, R. A. G., & Minow, N. (2011). *Corporate Governance* (5ª Ed.). London: Ed. Wiley.

Oliveira, C. L. (2010). Um apanhado teórico-conceitual sobre pesquisa qualitativa: tipos, técnicas e características. *UNIOESTE. Revista Travessias*, 3(3).

Porter, M. E. (1991). *Estratégia competitivas, técnicas para análise de indústrias e da concorrência* (16 ed.). Rio de Janeiro: Ed. Campus.

Porter, M. E., & Montgomorey, C. (1995). *Estratégia: a busca da vantagem competitivas*. Rio de Janeiro: Ed. Campus.

RMA – Risk Management Association. *Operational risk: the next frontier. The Journal of Lending & Credit Risk Management*. Recuperado em 26 setembro, 2015, de http://logicmanager.com/pdf/operational_risk_management.pdf

Sêmola, M. (2003). *Gestão da segurança da informação: uma visão executiva.* Rio de Janeiro: Ed. Campus.

Shea, E. P. (2006). Establish operational risk and compliance management as a sustainable business process. *Business Credit*, *8*(5), 16.

Trapp, A. C. G., & Corrar, L. J. (2005). Avaliação e gerenciamento do risco operacional no Brasil: análise de caso de uma instituição financeira de grande porte. *Revista Contabilidade finanças*. *16*(37), 24-36.

Yin, R. K. (2006). *Estudo de Caso – Planejamento e Métodos* (3ª ed.). Porto Alegre: Ed. Bookman.