Refas
Revista Fatec Zona Sul
1ª. Edição Outubro de 2014

GOVERNANÇA CORPORATIVA E A GESTÃO DE CONTINUIDADE DE NEGÓCIOS: ESTUDO DE CASO MÚLTIPLO EM EMPRESAS DO SETOR FINANCEIRO BRASILEIRO

CORPORATE GOVERNANCE AND BUSINESS CONTINUITY MANAGEMENT: A MULTIPLE CASE STUDY IN BRAZILIAN FINANCIAL INDUSTRY COMPANIES

GOBIERNO CORPORATIVO Y GESTIÓN DE CONTINUIDAD DE NEGOCIO: ESTUDIO DE CASO MÚLTIPLE EN EMPRESAS DEL SECTOR FINANCIERO BRASILEÑO

Alessandro Marco Rosini[1]
Rolf Henrique Neubarth[2]

Artigo recebido em junho de 2022
Artigo aceito em dezembro de 2022

DOI: https://doi.org/10.26853/Refas_ISSN-2359-182X_v09n05_02

RESUMO

As instituições do sistema financeiro brasileiro são pressionadas, por parte dos investidores, a aumentarem a eficiência operacional. Essas instituições tornam-se dependentes de plataformas tecnológicas, que precisam estar disponíveis, pois o risco operacional decorrente de indisponibilidades potencializa perdas financeiras significativas. A criação de uma gestão de continuidade de negócios eficaz permite a execução de um plano de resposta a eventos de alto impacto, indicando métodos, métricas e ferramentas para momentos de crise. Assim, este estudo tem como objetivo analisar a capacidade das empresas do setor financeiro para responderem a eventos de crises e de total parada em suas operações, atendendo aos requisitos específicos da NBR ISO/IEC 22301. Neste estudo de casos múltiplos, propomos uma coleta de informações, com entrevistas semiestruturadas, junto a uma amostra de cinco instituições do segmento financeiro, localizadas em Brasília e São Paulo e que aplicam *frameworks* de boas práticas de gestão de negócios e governança corporativa.

Palavras-chave: Governança Corporativa. Gestão de Risco. Gestão de Continuidade de Negócios. Instituições Financeiras.

[1] Professor e pesquisador, doutor em Comunicação e Semiótica, PUC SP e pós-Doutor em Administração de Empresas, FEA USP. E-mail: alessandro.rossini@yahoo.com. Lattes: http://lattes.cnpq.br/5109240355917713. Orcid: https://orcid.org/0000-0002-5150-8483.
[2] Executivo da área de TI, professor e mestre em Governança Corporativa. E-mail: henrique.fgvti@gmail.com. Lattes: http://lattes.cnpq.br/7202958540543486. Orcid: https://orcid.org/0009-0009-7248-7392.

ABSTRACT

Stakeholders demand entities within the Brazilian financial system to improve the operational efficiency since the risk management is critical to the business and to the technology platforms in operation. These platforms need to be always available with no disruptions. The creation of an effective business continuity management, with a high impact events response plan includes specific points and reports on business communication, indicating methods, metrics, and tools for actions at times of crisis. This article aims to analyze the ability of Brazilian financial industry companies to respond to failures and interruption at their sites, meeting the specific requirements from NBR ISO/IEC 22301. Thus, in these multiple cases study, we propose to collect information through a semi-structured interview with a sample of five institutions in the financial segment in Brasília and São Paulo, holding a framework of best practices in business management and corporate governance.

Keywords: Corporate Governance. Risk Management. Continuity of Business Management. Financial Institution.

RESUMEN

Las instituciones del sistema financiero brasileño están presionadas por los inversores para elevar la eficiencia operativa. Estas instituciones se vuelven más dependientes de las plataformas tecnológicas, que deben estar siempre disponibles, ya que el riesgo operacional derivado de la indisponibilidad aumenta pérdidas financieras. La creación de una administración eficaz de la continuidad del negocio permite la ejecución de un plan de respuesta a eventos de alto impacto. Así, este estudio tiene como objetivo analizar la capacidad de las empresas de la setor financiero para responder a eventos de crisis y tiempo de inactividad en sus operaciones críticas, cumpliendo con los requisitos específicos de NBR ISO / IEC 22301. Esta investigación és uno caso de estudio múltiple y se propone recolectar información, con entrevistas semiestructuradas, junto en una muestra de cinco instituciones del setor financiero, ubicadas en Brasilia y São Paulo, que aplican buenas prácticas en gestión empresarial y gobierno corporativo.

Palabras clave: Gobierno Corporativo. Gestión de riesgos. Gestión de la continuidad del negocio. Instituciones financieras.

1 INTRODUÇÃO

O fortalecimento de estratégias para utilização de tecnologias digitais, derivado da demanda crescente por modelos de negócios inovadores, visa o aumento de portfólio de negócios virtuais e a melhoria na eficiência operacional. Esse fator desenvolveu nas empresas do setor financeiro brasileira a dependência por plataformas tecnológicas, que precisam estar disponíveis e capacitadas para não apresentarem interrupções significativas. Com isso, essas empresas constantemente lidam com o risco potencial de perdas decorrentes de falhas operacionais, majoritariamente associadas à disponibilidade tecnológica.

Devido à dependência tecnológica e aos modelos de negócios interligados globalmente, as empresas são pressionadas, pelos investidores e usuários, a aumentarem a eficiência operacional e, consequentemente, a gestão de risco. Esse quadro, associado aos rígidos controles aplicados pelos órgãos reguladores das instituições financeiras, faz com que a adoção de práticas de governança corporativa combinadas seja necessária, para uma eficiente gestão de risco operacional e continuidade de negócios (BEAL, 2015). Esse plano deve estar contido na gestão do risco operacional da empresa, que pode ser definido como parte do escopo existente de uma governança corporativa (BEAL, 2015).

O risco operacional pode incorrer direta ou indiretamente em perdas inesperadas, devido às possíveis falhas ou ineficiência das pessoas, das plataformas tecnológicas, dos sistemas de informação, ou de controles internos de uma instituição. Resultantes de um impacto operacional, também existem perdas financeiras ou à não execução de operações de liquidação financeira que podem levar a processos jurídicos, perda de reputação, perda de imagem, multas de reguladores, danos ao ambiente e até à quebra da instituição (WALLACE; WEBBER, 2017; PEDOTE, 2002).

Segundo o BACEN – Banco Central do Brasil (2015), existem riscos que as instituições financeiras autorizadas a funcionar no Brasil devem considerar, em adequação aos princípios da Basileia Pilar 3 (acordo da Basileia III, de 17/08/1994, pelo Conselho Monetário Nacional). Pelo acordo, iniciou-se o desenvolvimento e a implementação de recomendações divulgadas, por meio da Resolução CMN nº 2.099. A Resolução CMN nº 2.554, de 1998, determinou que todas as instituições que operam no sistema financeiro brasileiro e demais instituições autorizadas pelo Banco Central deveriam implantar controles internos voltados para as atividades por elas desenvolvidas. A NBR – ISSO/IEC 22301 de 2013, estabelece a continuidade de negócios, guiando a implementação, direcionamento e monitoramento de um sistema de gestão documentado para a proteção da interrupção de operações (ABNT, 2007, 2013). Assim se faz uma empresa forte, com políticas de manutenção de segurança dos dados e eficiência das operações (PORTER; MONTGOMERY, 1998). Ainda, é importante delimitar quais os métodos alternativos de realização de operações, as plataformas de missão crítica e quem são os principais fornecedores na cadeia de fornecimento de serviços, pois estes pontos permitem entender como mitigar possíveis perdas derivadas de impactos operacionais (ALEVATE, 2014; WALLACE; WEBBER, 2017).

Como justificativa para este estudo, considera-se a importância da análise da gestão de continuidade de negócios e da capacidade de resposta, em tempo adequado, a eventos de alto impacto operacional em instituições financeiras que se defrontam com uma alta demanda por resultados por parte dos acionistas. Deve-se levar em conta a possibilidade de perdas potenciais em operações dessas empresas, devido às falhas operacionais e de gestão financeira. De acordo com o relatório da empresa Economatica (2016), a Receita Operacional Líquida (ROL) das empresas de capital aberto no Brasil caiu percentualmente 7,64% em 2015. Portanto, falhas tecnológicas que impactem os resultados se tornaram inadmissíveis, posicionando as empresas como grandes interessadas na gestão adequada dos próprios recursos tecnológicos, enquanto um ativo estratégico para a organização.

Depois de aprofundada pesquisa sobre os construtos e temas pertinentes, foi estabelecida a pergunta da pesquisa: as empresas da indústria financeira brasileira atuam com a gestão de continuidade de negócios e se preparam para responder a incidentes e eventos de alto impacto operacional quanto aos requisitos específicos da NBR ISO/IEC 22301? Nesse contexto, este estudo tem como objetivo analisar a capacidade das empresas da indústria financeira em responder a evento de crises e de total impacto ou indisponibilidade em seus *sites* principais de operação, atendendo aos requisitos específicos da NBR ISO/IEC 22301.

Para responder à questão e atingir o objetivo proposto, foi conduzido um estudo qualitativo, com análise de conteúdo e um roteiro semiestruturado de entrevistas com os gestores de riscos operacionais, de segurança da informação e de continuidade de negócios de cinco empresas financeiras de perfis e portes diferentes nas cidades de Brasília e São Paulo. Para composição do questionário, foram feitas entrevistas com especialistas nas disciplinas de Risco Operacional e Gestão de Continuidade de Negócios. Ainda, fez-se a análise de documentos (auditoria, análise de impacto do negócio, planos de recuperação de desastres ou

continuidade, processos de gerência de versões de mudança de tecnologia, de resultados de testes de planos de continuidade e de governança, políticas, procedimentos e memorandos).

2 REFERENCIAL TEÓRICO

No referencial teórico se abordam as práticas de governança corporativa que possam contribuir com o tema no setor financeiro, bem como a gestão do risco organizacional, importante e relevante para as questões relacionadas com o setor em discussão.

A gestão de continuidade de negócios e a gestão da tecnologia da informação também são abordadas no referencial teórico, pois são elementos fundamentais para segurança de qualquer tipo de organização.

2.1 Práticas de governança corporativa

McCahery, Sautner e Starks (2016) definem a governança corporativa (GC) como um conjunto de determinações dos usos gerais a que os recursos organizacionais estão submetidos e da totalidade de resoluções de conflitos entre todos os participantes nas organizações. De acordo com a Comissão de Valores Mobiliários (CVM, 2002), a definição de governança corporativa compreende um conjunto de boas práticas para que o desenvolvimento de uma companhia seja garantido, com facilidades de acesso ao capital investido e proteção aos investidores e aos funcionários. O código norte-americano de GC incorporou itens e estabeleceu seu próprio conjunto de normas ao código pioneiro, idealizado no Reino Unido, tais como: a) as obrigações de um conselho diretor de empresa pública na indicação e supervisão de seus CEOs; b) responsabilidade do gerenciamento operar a empresa de modo ético; c) apontamento da obrigação da gestão, junto com o conselho diretor, na produção de relatórios assertivos sobre finanças e os resultados; d) é responsabilidade do conselho e do comitê de auditoria contratar uma empresa independente para analisar a prestação de contas e verificar sua adequação aos princípios gerais de aceitação de contas (*Generally Accepted Accounting Principle* - GAAP) americano (TRICKER; TRICKER, 2015).

Dentro da vasta área de GC, os controles, procedimentos, planos e relatos de operações, processos para minimização da falha e do erro e o apoio à continuidade e gestão do risco encontram seus principais estudos e aplicações gerenciais (RIBEIRO et al., 2012; MECKLING, 2015). Dessa forma, cabe aos gestores e profissionais em geral, ao conhecerem as teorias de governança, adotarem pontos de vista e aderirem ações de implementação de boas práticas em consonância com a realidade existente (HERMALIN, 2014; MECKLING, 2015; TRICKER; TRICKER, 2015; MILES, 2017).

A implantação dos preceitos de governança abrange os conceitos específicos da área, a adaptação às normas da legislação própria dos setores, a associação do começo dos projetos de governança corporativa em inícios de mandatos governamentais, a profissionalização dos conselhos e o resguardo da influência político-partidária na empresa. Idealmente, há uma proposição de governança corporativa relacionada à transparência em contas e aos padrões uniformes de registro contábil (DE ABREU CAMPANÁRIO *et al*., 2014). Quanto mais unidades de negócios uma empresa possui, maior será o nível de complexidade ao qual está exposta. Múltiplas unidades de negócios estão focadas em produtos de mercado diversos, mas

precisam também estar conectadas entre seus setores e unidades (EISENHARDT; PIEZUNKA, 2011).

A responsabilidade social e a adaptação às mudanças ambientais são preceitos valiosos (OLIVEIRA; FORTE, 2009; LUNARDI et. al., 2016). No cenário brasileiro, as empresas se orientam pelos princípios básicos da governança corporativa, segundo o Código de Boas Práticas de Governança Corporativa, publicado pelo Instituto Brasileiro de Governança Corporativa (IBGC, 2015; FEBRABAN, 2019). São eles: transparência (disponibilidade de informações às partes interessadas), equidade (tratamento justo a todos os *stakeholders*), prestação de contas (ordem social, ambiental e definição de negócios) e a responsabilidade corporativa.

2.2 Gestão de risco operacional

As instituições financeiras, apenas por desempenharem sua função básica, que consiste em intermediar recursos financeiros, estão gerenciando riscos de crédito, riscos de mercado e riscos operacionais. Assim, risco operacional é o risco de perdas que foram geradas nos processos internos ou sistemas que falharam devido a eventos, internos ou externos, que não foram tratados (PEREIRA, 2004; WANG; XU, 2015; CHAVEZ-DEMOULIN; EMBRECHTS; HOFERT, 2016).

Visando atuar em aspectos de gestão de risco como foco para uma estratégia capaz de apoiar as organizações, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, 2011) publicou o documento *Internal Control – Integrated Framework*, em apoio a instituições que buscam um aperfeiçoamento em seus processos de gestão de controle e risco operacional. O COSO (2011) é formado por representantes da *American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Internationl, Institute of Managements Accountants* e pelo *Institute of Internal Auditors*, ao qual está ligado o AUDIBRA – Instituto dos Auditores Internos do Brasil, pela FLAI – Federação Latino-Americana de Auditores Internos. A premissa inerente do COSO é que toda organização existe para gerar valor às partes interessadas que, mesmo assim, enfrentam riscos e incertezas inerentes as suas demandas de operações. No que tange à gestão de continuidade de negócios, o COSO (2011) apoia, entre outras funções, a identificação, avaliação e respostas ao risco corporativo operacional, com uma rápida resposta a eventos de alto impacto, ver Quadro 1.

Quadro 1 – Riscos Operacionais

Identificação	Descritivo
Risco de Mercado	Risco de possibilidade de perdas decorrentes de flutuação nos valores de mercados, riscos de operações financeiras sujeitas a reajustes cambiais, taxas de juros e precificação de ações e *commodities*.
Risco de Liquidez	Risco decorrente da instituição por ter sua capacidade de pagamento impactada ou seus recebimentos em possível desequilíbrio dos ativos que podem ser negociados.

Risco Operacional	Riscos associados à ocorrência de perdas derivadas de falhas sistêmicas, falhas em processos internos ou ocasionados por incidentes de eventos externos associados ou não às inadequações de operações, que não podem ser executadas devido a uma interrupção nas operações da instituição.
Risco de Crédito	Risco de possibilidade de perdas decorrentes de flutuação nos valores de mercados, riscos de operações financeiras sujeitas a reajustes cambiais, taxas de juros e precificação de ações e *commodities*.

Fonte: os autores, baseado em Pedote (2002)

Nos controles da gestão do risco, entram aspectos de várias disciplinas, como segurança da informação, tecnologia da informação e finanças (PEDOTE, 2002; STEINBERG, 2016). O Quadro 1 mostra a descrição dos tipos de riscos operacionais enfrentados pelas empresas, também orientados pelo Conselho Monetário Nacional - CMN (2015) e pelo Banco Central do Brasil - BACEN (2015)

2.3 Gestão de continuidade de negócios

Segundo a ABNT NBR 15.999-1, gestão de continuidade de negócios pode estar relacionada a um processo de gestão, que visa identificar as ameaças potenciais para uma organização e, dessa forma, estabelecer os impactos nas operações de negócios. Gestão de continuidade de negócios é uma responsabilidade da organização como um todo, especialmente no que diz respeito à infraestrutura de TI, que impacta diretamente operações de missão crítica da empresa (LUNARDI et al., 2016).

A metodologia de base para a gestão da continuidade de negócios está descrita tanto na atual NBR/ISO 22301 (ABNT, 2013) como na norma originária BS 25999-2 e na norma brasileira NBR 15999, criada em 2008, para orientar sobre o assunto. A base estabelece: a) planejar o projeto conhecendo seus objetivos; b) atribuir estudos de região, áreas, riscos pertinentes à situação; c) mensurar e documentar todos os impactos do cenário, situação, quando problema não for resolvido; d) determinar plano estratégico ou modelo de atuação para contingência dos riscos identificados e estudados; e) criar e documentar planos de atuação, divididos por planos de negócio e planos físicos; e f) quando há possibilidade de crise, testar e comunicar todos os envolvidos no projeto as decisões que serão tomadas quando ocorrer um problema previamente estudado (ALEVATE, 2014).

A gestão de continuidade de negócio não pode ser uma política ou um plano elaborado, pois deve ser um processo de proatividade, com dinamismo e continuidade, por meio de revisões, atualizações e adaptações. Dessa forma, o planejamento da estratégia de recuperação evita que o incidente, caso ocorra, interfira na normalidade do funcionamento do negócio (BRITISH STANDARDS, 2006). Para que o plano de continuidade seja efetivo dentro das empresas, relacionam-se princípios claros para a gestão de continuidade de negócios, tais como estrutura, plano, escopo de plano de resposta, prioridade do crítico, atualização desses planos, comunicação com todos os pares e replicação de dados, com *backups* ou *storage* (WALLACE; WEBBER, 2017).

A norma BS25999 contém um conjunto de controles de segurança e práticas de gestão de segurança de informação, dividido em duas partes. A primeira parte consiste num código de práticas para segurança de informação. A segunda parte define um conjunto de especificações para sistemas de gestão de segurança de informação, o que levou a norma a ser submetida à ISO, motivando a publicação da norma ISO/IEC 17799. O sistema de gestão da segurança da informação (*Information Security Management System*) preocupa-se com a gestão de confidencialidade, integridade e disponibilidade da informação, indicando que devem ser identificados todos os riscos de interrupção nas atividades de negócio – ISSO/IEC 27002. Já a NBR/ISO 22301 é um conjunto de requisitos padrão de sistemas de gestão que descreve como alcançar uma boa prática para a continuidade dos negócios, presente em 45 países. Publicada em 2012 (ABNT, 2019), aplica um modelo "*Plan-do-check-Act*" (PDCA) para planejar, estabilizar, implementar, operacionalizar, monitorar, revisar e melhorar a eficácia da gestão de continuidade de negócios da organização.

2.4 Gestão de Tecnologia da Informação

Um dos principais objetivos da governança corporativa é criar mecanismos eficientes de gestão, monitoramento e a adoção de controles e métricas para garantir as metas determinadas pela organização, dando apoio aos executivos, alinhando processos e as operações da empresa com os interesses dos investidores e demais *stakeholders.* Essas ações garantem os investimentos dos acionistas e possibilitam atender aos processos de regulamentação da indústria tanto para a organização quanto para suas disciplinas, como a Tecnologia da Informação (TI) (LIU; ZHANG, 2017). As organizações não conseguem implementar uma governança corporativa sem a adoção de boas práticas de tecnologia da informação. Assim, a governança de TI consegue atrelar os objetivos da organização com a efetiva monitoração das atividades corporativa, provendo o devido suporte aos aspectos operacionais requeridos (CUI et al., 2015). Quanto a isto, podem ser citados o apoio das plataformas, aplicativos, utilitários e sistemas, aos conselhos administrativos, diretorias, comitês fiscais e auditorias internas e externas.

Incluem-se, nos controles de informação, procedimentos de desenvolvimento de sistemas de informação, aquisição de ativos de tecnologia, gestão de recursos de conectividade e armazenamento de base de dados relacionados a informações financeiras (CUI et al., 2015). Com isso, adotar uma boa prática de gerenciamento de serviços de tecnologia de informação é essencial para operar no mercado financeiro. As empresas só são capazes de superar seus concorrentes se conseguirem estabelecer uma diferença que possa ser sustentada (PORTER; MONTGOMERY, 1998). Sobre a gestão de Tecnologia da Informação, Fagundes (2012) define o ITIL – *Information Technology Infrastructure Library* como um dos modelos de gestão para serviços de suporte à infraestrutura mais adotados pelas organizações ao redor do mundo. O ITIL é um modelo não proprietário, que define as melhores práticas para o ciclo de gerenciamento dos serviços de TI. O ITIL é um conjunto de recomendações baseadas em boas práticas de Gerenciamento de Serviços de Tecnologia da Informação. O ITIL encontra-se na versão 3 e descreve cinco ciclos de vida: a) *Service Strategy* (Estratégia de Serviço); b) *Service Design* (Delineamento do Serviço); c) *Service Transition* (Transição de Serviço); d) *Service Operations* (Operação de Serviço); e e) *Continual Service Improvement* (Processo de Melhoria Continuada de Serviço). Portanto, uma Gestão de Continuidade de Negócios não consegue ser realizada sem que a definição de impactos nos serviços de tecnologia da informação seja claramente definida.

3 MÉTODO

Nesta pesquisa, foram realizadas entrevistas roteirizadas para uma maior interação entre as partes envolvidas. As entrevistas foram realizadas no ano de 2017 e a análise de conteúdo trouxe uma possibilidade relevante de investigação da pesquisa, designando a verificação dos conteúdos obtidos durante os processos de coleta de dados (BARDIN, 1977; COOPER; SCHINDLER, 2016).

3.1 Delimitação e amostra da pesquisa

A delimitação deste estudo considerou como unidades de observação para análise e coleta de dados a relação de instituições financeiras informadas no *site* do Banco Central do Brasil, que somam 600 (seiscentas) instituições financeiras brasileiras, divididas em: a) conglomerados; b) bancos comerciais, múltiplos e caixa econômica; c) cooperativas de crédito; d) bancos de investimento, bancos de desenvolvimento, sociedades corretoras, câmbio, sociedades distribuidoras de Títulos de Valores Monetários, sociedades de crédito, financiamento e investimento, sociedades de crédito imobiliário, entre outras. Neste caso, esta pesquisa visou identificar se as empresas possuem Gestão de Continuidade de Negócios, dentro de um diagnóstico comparativo quanto à existência de uma gestão de continuidade de negócios nas empresas da indústria financeira que utilizam como melhor práticas aspectos da norma NBR ISO/IEC 22301.

Dessa forma, foram abordadas cinco empresas de perfis e portes diferentes, com operações distintas, mas que seguem as regulamentações estabelecidas pelo regulador principal. A diversificação das unidades-caso pesquisadas foi considerada como fator fundamental para a ampliação da visão do tratamento do risco operacional. Dentre as empresas selecionadas, três são bancos e duas operam como empresas de corretagem de valores e seguros. Nesta pesquisa, tratamos cada instituição por uma letra do alfabeto. A instituição A é um banco multinacional com capital de origem estrangeira com sede em Nova Iorque e 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 Iorque, que não possui operação de varejo no Brasil e opera somente no mercado corporativo financeiro, com uma crítica operação de *trade* e produtos financeiros para grandes clientes e corporações no consórcio brasileiro. A terceira 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 em termos de alcance operacional, com operação centralizada em São Paulo, e a instituição E é uma corretora de seguros multinacionais de médio porte, com forte presença nas operações dos países da América Latina e com foco em seus principais mercados, como Brasil e Argentina.

3.2 Instrumentos de pesquisa e procedimentos de análise de dados

Para um estudo aprofundado que permitisse um nível de detalhamento dos procedimentos adotados, permitindo se estabelecer uma coleta de dados, os instrumentos de pesquisa utilizados neste estudo foram: a) entrevistas abertas com os gestores de riscos operacionais das instituições, com os gestores de Segurança da Informação ou Gestão de Continuidade de Negócios, com os gestores de Tecnologia da Informação e com especialistas nas disciplinas de Risco Operacional e Gestão de Continuidade de Negócios; b) utilização de dados secundários; c) análise de documentos de auditoria; d) *Business Impact Aanalysis*

(Análise de Impacto do Negócio); e) planos de Recuperação de Desastres ou continuidade de negócios; f) processos de gerência de versões de mudança no ambiente de tecnologia, ou análise de documentos, que evidencie o controle do ambiente de versões técnicas; g) análise de resultado de testes de Plano de Continuidade de Negócios; h) políticas de Gestão de Continuidade de Negócios; e i) documentos de governança, políticas, procedimentos e memorandos.

Um teste do instrumento de entrevista foi realizado com uma das unidades-caso em dezembro de 2016. Após a validação dos instrumentos (questionário e abordagens de diálogo), procedeu-se às entrevistas com os profissionais das cinco empresas financeiras, a saber, responsáveis, gerentes e diretores das áreas de gerenciamento de continuidade de operações e governança corporativa. Dentro do roteiro, considerou-se a possibilidade de um evento ou incidente que impactasse as operações das instituições e a existência de mecanismos e processos. Como parte da análise da resiliência das empresas pesquisadas, buscou-se o apoio na boa prática de gestão de continuidade de negócios da NBR ISO 22301.

3.3 Instituições da pesquisa

Iniciam-se os detalhamentos das instituições pela Instituição A.

3.3.1 Instituição A

O gestor da área de Continuidade de Negócios da instituição A se dispôs a receber a entrevista virtualmente, em *site* próprio da empresa. A Governança de Risco Operacional é conduzida, na empresa, por quatro funcionários, os quais se apresentam certificados na disciplina e atuam integralmente na Gestão de Continuidade de Negócios. Há uma política específica sobre o tema de continuidade de negócios, o que possibilita a disseminação do conhecimento entre os diversos níveis da companhia. Além disso, existe a discriminação dos níveis críticos e equipes-chave envolvidas no processo de continuidade de negócios, permitindo a identificação e o alinhamento para o adequado desenvolvimento de planos em casos de recuperação de desastres. Conforme informado pelo gestor de continuidade, os testes de risco da empresa abrangem teste: a) operacional; b) de ensaio em plano tático; c) de especificidade de componente crítico; e d) de plataformas (componentes para continuidade de negócios).

As áreas de negócio podem participar, validando a execução dos testes e fornecendo dados que permitem analisar o sucesso do teste ou as oportunidades de melhorias no processo, por meio da coleta de evidências, como telas de sistemas e lançamentos simulados em bases específicas para aplicação do teste. Por meio das simulações, é possível medir o RTO - *Recovery Time Objetive* (Objetivos de Tempo de Recuperação), que é o tempo esperado para ativação de um plano de contingência, após a informação de que há uma situação de alto impacto nas operações. A Governança de TI e a Segurança da Informação, efetivamente, apoiam a disciplina de risco operacional, por meio da adoção das boas práticas defendidas no *framework* do ITIL. Foi possível identificar que a Gestão de Mudanças é claramente definida em processos que são seguidos pelas áreas de desenvolvimento e infraestrutura.

A empresa A disponibilizou, para esta pesquisa, um documento classificado como "Política de Gestão de Tecnologia". O documento completo está divido em Políticas Relacionadas à Conformidade, Política de Governança, Gestão de Tecnologia da Informação de Risco e Política de TI. A área de Infraestrutura de Tecnologia da informação desta instituição financeira possui uma área de Gestão de Mudança, dedicada a avaliar todo e qualquer processo de mudança nas plataformas de TI. Dentro deste escopo de análise, o gestor da área de

Mudanças de Tecnologia da Informação fica como principal responsável por conduzir reuniões, das quais participam áreas de tecnologia. Sob o aspecto operacional, observou-se que o Comitê de Gestão de Mudanças passou a adotar práticas mais rígidas, para que as mudanças submetidas passassem a ter um plano claro e conciso para executar atualizações no ambiente, garantindo que todos os *stakeholders* estivessem envolvidos na decisão de "ir" ou "não ir" com a mudança, garantindo que exista o máximo de mitigação de riscos na sua execução.

Durante a pesquisa e análise realizada na empresa A, observou-se que, uma vez que esse processo de mudança seja obedecido e seguido corretamente, com todas as documentações atualizadas, a tendência de se ter um incidente derivado de uma mudança é reduzida significativamente. Como citado, há garantia de que outros ambientes estejam atualizados ao mesmo tempo em que uma atualização ou algum *update* crítico seja realizado.

Nesta pesquisa, identificou-se que a empresa classifica a severidade, de acordo com as manobras de continuidade de negócios, em alta severidade, média severidade e baixa severidade das operações (na qual a manobra de recuperação não interfere nas operações). Para a recuperação, há o *Recovery Time Objective* – RTO. Segundo o entrevistado da empresa A, os eventos ou incidente já identificados ao longo das manobras de testes podem ocorrer pelos seguintes motivos: a) falta de atualização de versão entre ambientes; b) execução de atualização e mudança nos sistemas tecnológicos – erros causados por demandas de atualizações de sistemas; c) erro operacional causado por operação humana seja por desenvolvedor de sistema, suporte técnico ou erro de operação de ambiente como as rotinas de *datacenter*; d) falha de *hardware* de equipamentos de infraestrutura de tecnologia que podem interromper a disponibilidade dos ambientes; e) erro nos processos de *script* que instruem como recuperar uma aplicação, sistema ou plataforma; e f) erro na recuperação de dados do *backup* ou erro no processo de restauração dos dados.

Na empresa A, a Gestão de Problemas e Incidentes se ampara na identificação de SPOFs (*single point of failure*), com componentes ou plataformas intolerantes a falhas, devido à ausência de uma estrutura de redundância, o que pode impactar e causar um risco para as operações da instituição. Além disso, há espelhamento *hot swap* de servidores, base de dados e plataformas. Toda a infraestrutura do *site* de contingência é ativo fixo da empresa e é dedicada à continuidade de negócios, sendo que a instituição detém o investimento necessário para manutenção da infraestrutura de contingência ativa e devidamente atualizada.

A instituição A atua com a adoção de controles internos de *Risk Control Self Assessment*, utilizado pelo mercado e apoiado pela interseção com a disciplina de segurança da informação, demonstrando que a gestão de governança de risco operacional dispõe de uma alta maturidade. A instituição executa duas vezes ao ano um exercício que considera a queda do site principal de operação e a recuperação dos processos essenciais no *site* de contingência, realizando as validações dos RTOs junto às áreas usuárias dos serviços. A instituição retém significativos investimentos para garantir o nível de maturidade, a adequada governança e segurança da informação, possuindo um alto grau de resiliência em sua operação.

3.3.2 Instituição B

A instituição B, igualmente representada pelo Gestor de Continuidade de Negócios da empresa, dispôs-se a responder a pesquisa pelo telefone, meio pelo qual foi possível identificar os pontos descritos. A Governança de Risco Operacional conta com a atuação de três profissionais, dedicados para a gestão de continuidade de negócios, dentre eles, o gestor de risco operacional. Apesar de apresentar uma operação menor que a instituição A, no tangente ao volume de processamento realizado, a aplicabilidade e gestão de continuidade de negócios

da instituição B é equivalente à da instituição A. Os funcionários são igualmente certificados e treinados na disciplina de gestão de continuidade de negócios. A principal diferença, no tocante à gestão de continuidade de negócios, entre as instituições A e B, está na realização dos testes de continuidade de negócios, pois a instituição B adota o conceito de que a execução do teste consiste apenas no acesso ao sistema, dispensando a validação de lançamentos sistêmicos. Assim, não há a garantia efetiva do funcionamento correto dos sistemas tecnológicos em um cenário de completa indisponibilidade do *site* principal.

A Governança de TI e de Segurança da Informação na instituição B demonstrou ser estruturada dentro dos padrões similares ao aplicado na instituição A, detendo o mesmo modelo de interseções com as disciplinas de gestão de problemas e incidentes e gestão de mudanças. Foram apresentadas informações, durante a entrevista, sobre a existência de um comitê de Risco Operacional. A instituição B detém um *site* alternativo, com posições de trabalho capacitadas com a infraestrutura tecnológica necessária para operacionalização de funcionários. A tecnologia para replicação de dados críticos considera os seguintes pontos, avaliados durante a entrevista: a) espelhamento de servidores; b) base de dados; c) plataformas e replicação de telecomunicações, de forma a balancear a carga de tráfego de dados. Neste caso, a premissa é de que o tráfego de dados seja feito simultaneamente em ambas as conexões. Ou seja, há a utilização da abordagem dupla, por meio do uso conjunto de roteadores e operadoras de serviço, visando assegurar a disponibilidade de acesso do tráfego de dados, em um *site* contratado no mercado. O grau de maturidade da empresa B, promovido pela governança de processos de TI, também pode ser considerado alto, dada a aplicação de políticas para continuidade de negócios e segurança da informação, disseminados em todos os níveis hierárquicos da companhia. Tal ação possibilita o desenvolvimento de testes que validem toda a cadeia de processos críticos da companhia pelo time de gestão de risco operacional, propiciando o tempo de resposta requerido no RTO – *Recovery Time Objetive* (Objetivo de Tempo de Recuperação), atendendo às expectativas dos acionistas no contorno de um evento de crise de grandes proporções.

Apesar do risco inerente na adoção de um site compartilhado de posições de negócio para utilização em um plano de contingência, é possível afirmar que há um alto grau de resiliência na operação da instituição B. Inclusive, uma vez ao ano, é executado um exercício para testar a recuperação dos principais processos no site de contingência, após a queda do *site* principal de operação, validando junto às áreas usuárias a recuperação de acessos e verificando o atendimento às expectativas dos RTOs estipulados. Outro ponto a ser explanado, sobre as diferenças entre as instituições A e B: a estrutura de *site* alternativo utilizado pela segunda evidencia a diferença na gestão de risco *versus* o investimento em um *site* dedicado, pois, apesar de menor, há dispêndio financeiro, devido à utilização do modelo de *co-location*. A operação considera o custo para construção da infraestrutura tecnológica necessária para garantir a operacionalização de negócios de uma instituição financeira. A locação e a utilização do espaço empregadas no modelo de *co-location* da instituição B devem ser claramente definidas e monitoradas, visando garantir a disponibilidade de serviços.

O entrevistado da instituição B informou a existência de um documento BIA, no qual os processos são classificados por impacto financeiro. Porém, declarou também não poder apresentar ou disponibilizar esse documento por conter questões de confidencialidade de informações e por endereçar processos de negócios e o envolvimento de valores de negócios. A instituição B possui também, em seus planos de recuperação de desastres, as informações necessárias sobre seus principais fornecedores mais críticos, que precisam estar disponíveis em caso de uma declaração de contingência. Entretanto, não informou onde essa informação estaria disponibilizada dentro do plano de recuperação de desastres. Dentro do construto de risco operacional e gestão de continuidade de negócios, o entrevistado afirmou que o único fornecedor crítico informado foi o *datacenter* de terceirização de processamento de dados. A

instituição B apresentou um bom nível de maturidade em governança corporativa, de gestão de risco operacional e gestão de continuidade de negócios, utilizando a NBR ISO 22301.

3.3.3 Instituição C

A instituição C possui grande porte e alcança apenas o cenário nacional, atuando exclusivamente no varejo do segmento bancário. A entrevista, assim como ocorreu na instituição B, foi conduzida por telefone com o Gestor de Continuidade de Negócios, o que permitiu a análise dos pontos a seguir descritos. O gestor disponibilizou dados secundários que, segundo ele, foram classificadas como informação pública e que serviram de base de consolidação para a utilização do estudo. Devido ao formato de atuação, a instituição dispõe de áreas em prédios diferentes, podendo descentralizar operações críticas e áreas de negócios, aumentando as oportunidades para criação de cenários de recuperação em caso de desastres. O entrevistado relatou a existência de três prédios, sendo que a replicação dos dados é feita entre dois deles, utilizando-se soluções de alta disponibilidade de replicação de dados para a estratégia de recuperação. A área de governança de risco operacional conta com oito funcionários que atuam na gestão de continuidade de negócios e apoiam outros processos, como a CIPA, a análise de segurança de perímetro e segurança do trabalho, por exemplo. Além da interação com a área de TI, os profissionais também revisam processos junto às áreas críticas do negócio. Contudo, diferente das instituições A e B, apenas o gestor é certificado em gestão de continuidade de negócios na instituição C. O modelo de governança para a continuidade de negócios é semelhante entre as instituições A, B e C, mantendo um elevado grau de maturidade, ao analisar possibilidades de impacto ao negócio, por meio da revisão crítica de processos.

Os processos indispensáveis para operação do negócio, denominados processos críticos, são devidamente mapeados e documentados. Processos que envolvem impactos financeiros são mapeados e armazenados em um sistema específico, contendo as informações sobre riscos operacionais. A instituição bancária C, assim como as demais instituições analisadas, possui *site* específico com posições de trabalho e com a replicação de toda a infraestrutura de TI. Ela também espelha base de dados, servidores, plataformas e telecomunicações, que contam com abordagem dupla, mas com a mesma operadora de serviço. Há roteadores distintos, visando garantir a disponibilidade de acesso de tráfego de dados, assim como a existência de dados de alta disponibilidade, mas todos providos por uma mesma operadora. Os documentos analisados foram: Política de Segurança da Informação e Política de Continuidade de Negócios da instituição C.

O *site* principal, no qual rodam as plataformas de negócios da empresa, abriga as áreas de negócio responsáveis pelo *core business* das operações de varejo. Os testes de acionamento do *site* de contingência são executados anualmente, considerando um cenário de total interrupção, com resultados documentados e assinados pelas áreas de negócios. Contudo, devido ao porte maior, em comparação com as instituições A e B, a instituição C possui uma estratégia diferenciada, contando com três *datacenters*, que não interagem de modo integrado entre si.

A empresa, segundo o entrevistado, possui políticas diferenciadas. Para recorte e delimitação deste estudo, o entrevistado foi questionado sobre a existência de uma política de Gestão de Continuidade de Negócios, segmentada para gestão de risco e plano de resposta a um alto impacto operacional. No caso de continuidade de negócios, o documento de recuperação de desastres traz diretrizes públicas, pois devem mostrar que estão aderentes a boas práticas de governança corporativa ao mercado e acionistas. A empresa possui uma agenda com um comitê, no qual participam funcionários estatutários e que é denominado de comitê de riscos. Na

empresa C, também há comitês de segurança de informação, nos quais há uma agenda para discussão de risco operacional, envolvendo gestão sênior, e que lidam, inclusive, com a análise e aprovação do BIA, sendo que, por exemplo, esse comitê aprova essas análises. A agenda desse comitê é mensal e há o grupo de gerenciamento de crise com o monitoramento desta disciplina. Conforme citado, a empresa C possui uma robusta infraestrutura de tecnologia da informação, na qual três centros de processamento de dados e telecomunicações existem e são operados para suportar ambientes de TIC e divididos do ponto de vista operacional de estratégia de gestão de continuidade de negócios.

Na empresa C, há dois dos três *datacenters* operando simultaneamente, mas estes não estão operando de forma paralela. Os centros de processamentos de dados primário e secundários estão a sete quilômetros de distância, com um próprio *design* de rede dedicado e com uma conexão de fibra ótica, proporcionando o *throughput* de dados em velocidade Giga, necessária para o devido suporte de replicação de dados, suportando um *back-to-back* de alta velocidade de transferência de dados entre os centros. Alguns serviços estão espelhados, mas só para alguns processos críticos. O entrevistado da empresa C informou que 17 processos de negócio existentes são considerados altamente críticos e são priorizados na criação dos planos de contingência e na estratégia de operações. Há um projeto de TI em andamento, para o qual há uma previsão de se implantar uma infra de contingência espelhada para todos os processos que estão em produção.

A estratégia de clusterização utilizada pela instituição C confere um grau maior de resiliência ao sistema, em comparação às instituições A e B, na recuperação das informações, mas não necessariamente no retorno da plataforma disponível ao negócio. Na possibilidade de existir um evento que impacte a operação, a instituição C está equipada com *sites* operantes para acolher profissionais que possam continuar a operação, mas requer um tempo de recuperação e preparação do ambiente de contingência.

3.3.4 Instituição D

A instituição D, que apresenta o menor porte entre as instituições em análise, foi representada pelo gestor de operações da empresa. Esse profissional não é certificado, não possui especialização nas áreas de risco operacional, tecnologia da informação ou gestão de continuidade de negócios. Seu *background* técnico é totalmente focado em negócios de corretagem de valores, mas ele acumula funções operacionais, *compliance*, segurança da informação e aspectos regulamentares. Dentro de uma análise do construto de governança corporativa e risco operacional, entende-se que a instituição D não possui profissionais dedicados à disciplina de gestão de continuidade de negócios ou governança de risco operacional, encarregados de ver que sua operação não comporta essa demanda. O formato de trabalho exibe a atuação de um auditor externo, que atua no chamado *on demand*, ou seja, que é contratado por meio de uma empresa de auditoria e que documenta as regulamentações para atender às disciplinas necessárias para operacionalização do negócio. Essas operações incluem a gestão de risco operacional e as entregas de informações dos órgãos reguladores, como Comissão de Valores Mobiliários e o Banco Central. Um auditor atua em parceria com o gestor de operações, que é o responsável por garantir a disponibilidade da infraestrutura essencial à operacionalização dos sistemas de *trader*, que são as plataformas diretamente relacionadas ao *core business* da instituição, o qual é formado pelas operações de corretagem de valores. Dentro de uma análise do construto de risco operacional, entende-se que as plataformas de *trader* dispõem de *softwares* utilitários, integrando informações sobre fundos de investimentos, operações financeiras, mercado da Bolsa de Valores de São Paulo – BM&FBOVESPA, carteira

de clientes e informações de mercado especializadas para tomada de decisão sobre compra e venda de títulos e demais informações pertinentes às operações dos *traders*.

Considerando as oportunidades da própria plataforma de t*rader*, a instituição D não possui um site alternativo dedicado, como as demais instituições em análise, que fazem espelhamento de servidores, plataformas, base de dados e telecomunicações, entre outros. Apenas a infraestrutura de TI é contingenciada, por meio de um *datacenter* contratado, que prevê a utilização de máquinas servidoras para recuperação de dados, pela restauração de *backups* e de plataformas de suporte ao negócio, a partir de mídias disponíveis no *site* contratado e que apoiam a contingência das operações. Executando o aspecto de conectividade, a instituição D possui um *link* de telecomunicações de velocidade de 20Mbytes de banda em tecnologia MPLS (*Multiprotocol Label Switching).*

A instituição D possui um processo de governança de TI com baixa maturidade, ou seja, processos de boas práticas não são necessariamente aplicados, devido ao seu universo tecnológico ser de pequeno porte, segundo informações do entrevistado. A segurança da informação fica a cargo das criptografias das plataformas de *trader*, que já são suficientes para garantir a confidencialidade das operações feitas em nível de *software*. Os sistemas críticos são contingenciados por meio de *backup* incremental, que é realizado diariamente, ou seja, somente a informação que é gerada no dia é copiada para as mídias de segurança e *backup*. Não há uma replicação dos sistemas, aplicações ou dos servidores que suportam as plataformas de negócios, sendo feita de forma sincronizada.

O entrevistado informou que testes de recuperação de *backup* são realizados num nível de análise de *log*, para verificar a consistência do *backup* de dados e que, recorrentemente, é demandado a restaurar *backups* para fins de operações rotineiras, mas que a recuperação existente é somente em nível de dados e não em nível de plataformas ou de recuperação de ambiente, tornando difícil avaliar que, em uma situação de alto impacto operacional, sua recuperação se dará em tempo adequado para as demandas do negócio.

Dentro de uma análise de risco operacional e gestão de continuidade de negócios, não há boas práticas de *frameworks*, como o ITIL, por exemplo, ou em nenhum nível de atuação da empresa, denotando-se a não existência de uma gestão de mudança ou o mapeamento de fornecedores críticos que estejam refletidos em um plano de recuperação. Há sim a gestão de fornecedores e contratos, mas somente em nível jurídico. O entrevistado disponibilizou documentos considerados como dados secundários, que evidenciam que há um plano de recuperação de desastres sendo confeccionado e com informações consideradas críticas para executá-lo. Há ainda a evidência de que haverá a aprovação deste plano, mas não há evidências sobre um teste sendo realizado com áreas de negócio em acordo com a ISO 22301.

3.3.5 Instituição E

A instituição E apresenta porte médio, em termos de plataformas tecnológicas entre as demais unidades casos investigadas. A empresa possui unidades no Rio de Janeiro, São Paulo e Minas Gerais, mas seu principal ponto de operações concentra-se em São Paulo e possui 330 funcionários distribuídos nesses escritórios. O Diretor de Operações e Tecnologia se dispôs a receber o entrevistador presencialmente. Com relação à governança corporativa, a instituição E possui políticas e processos que se desdobram para controles, que podem ser considerados indícios de uma governança corporativa bem estruturada. O entrevistado representa a diretoria de operações da empresa. A instituição E não possui profissionais dedicados à disciplina de gestão de continuidade de negócios ou governança de risco operacional, como se observou

também na instituição D, também pelo mesmo motivo indicado, pois sua operação não comporta essa demanda, devido à natureza de suas operações.

Dentro do escopo de atuação da empresa, é preciso considerar que um corretor de seguros atua como um profissional do ramo securitário tanto como profissional autônomo, pessoa física, quanto como pessoa jurídica, dentro do universo de produtos de uma corretora de seguros. O papel de uma empresa do ramo de corretagem de seguros é, principalmente, analisar custos e benefícios relacionados à situação de um cliente segurado, prospectando vendas na indicação de produtos de seguro. Devido a esse aspecto, tais serviços mencionados consistem, em sua maioria, na operacionalização e execução de ordens de venda de seguros. Com relação à tecnologia da informação, risco operacional e continuidade de negócios, a instituição E possui um *site* alternativo, contratado de um provedor de *datacenter*. Ainda possui posições de contingência para as áreas de negócio com um total de 40 posições de trabalho disponíveis em caso de necessidade de acionamento em uma situação de contingência, apesar de fazer espelhamento de dados.

A instituição E possui um processo de governança de TI com alta maturidade, ou seja, processos de boas práticas baseados na biblioteca de boas práticas do ITIL, mencionadas no referencial teórico deste estudo, são aplicados devido ao seu universo tecnológico ser de médio porte, segundo informações do entrevistado. As gestões de mudanças possuem controle de *release* e são devidamente certificadas pelo gestor de tecnologia da informação. Como a demanda por disponibilidade e a conexão externa são muito inferiores, se comparadas com as pertencentes às instituições A, B e C, a demanda por disponibilidade também é menor e limita-se ao período de funcionamento do sistema financeiro nacional. Os pontos de GC foram avaliados de acordo com o que se propõe a pesquisa, que sempre está veiculada às diretrizes da ISSO 22301.

A instituição E opera em um dos escritórios principais, localizado em São Paulo, um risco considerado significativo, pois foi possível identificar que o prédio não possui contingência para fornecimento de energia. Dentro da análise de GC, a recuperação existente nas manobras de testes e não ocorre somente em nível de dados, mas também há uma validação de conectividade em nível de plataformas ou de recuperação de ambiente. Esse fator é crucial para tornar a empresa mais resiliente, devido à avaliação de que, em uma situação de alto impacto operacional, sua recuperação se dará considerando seu RTO, em seu tempo adequado com as necessidades do negócio. Há processos e controles bem estruturados e boas práticas de *frameworks*, como o ITIL, por exemplo, constatando-se a existência de uma gestão de mudança ou o mapeamento de fornecedores críticos que estejam refletidos em um plano de recuperação em obediência à ISO 22301.

4 RESULTADOS E DISCUSSÃO

No Quadro 2, observam-se, resumidamente, os resultados empíricos obtidos nesta pesquisa e explicados a seguir. Nas colunas destinadas às empresas, há os resultados da análise que demonstram se cada instituição se encontra em alinhamento com as diretrizes da NBR ISO 22301.

Quadro 2 – Resumo dos resultados encontrados nas cinco instituições pesquisadas

Instituição	A	B	C	D	E
A organização possui política(s) específica(s) para o cumprimento de ações relacionadas à gestão de riscos, controles internos e sistema de conformidade (*compliance*)?	Sim	Sim	Sim	Sim	Sim
A diretoria da organização possui agenda específica na identificação de processos relacionados a riscos operacionais?	Sim	Sim	Sim	Sim	Sim
Há comitê(s) interno(s) de auditoria, de forma a estabelecer processos de monitoração interna, garantindo que os sistemas de controle adotem atitudes preventivas na gestão de risco operacional?	Sim	Sim	Sim	Sim	Sim
A organização possui uma área ou departamento para atuar em aspectos de gestão de risco operacional?	Sim	Sim	Sim	Sim	Sim
A organização possui um *datacenter* de produção e secundário ou alternativo para acionamento em caso de um impacto operacional?	Sim	Sim	Sim	Não	Sim
A organização possui GeMud que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas em contingência?	Sim	Sim	Sim, sem replicaçã o de sistemas.	Não	Sim,
A organização possui duplicação de abordagem de link de telecomunicação de dados entre seus principais sites de negócio?	Sim	Sim	Sim, com uma única operador a	Não	Sim
A organização possui uma política de GCN que provê um modelo de governança para gerir uma crise de forma ordenada. com foco em restaurar as operações do negócio na ocorrência de eventos de impacto?	Sim	Sim	Sim	Sim	Sim
A organização possui uma classificação de criticidade dos processos de negócio (Business Impact Analysis – BIA)?	Sim	Sim	Sim	Sim, com nível de baixo detalhament o	Sim
A organização possui procedimentos de recuperação de desastres das principais localidades incluindo ambientes e aplicações de TI com mapeamento de conectividade externa?	Sim, mas não TI legadas	Sim	Sim, mas somente com backup de dados	Sim, mas não é feita replicação de dados sincronizada	Sim

Executa os testes dos planos de continuidade de negócio?	Sim, porém sem cenários *End-to-End*	Sim	Sim, porém sem cenários *End-to-End*	Sim, porém somente tabletop	Sim
A organização possui a revisão e a coleta dos resultados dos testes e a criação de planos de ação para corrigir os problemas ocorridos durante as manobras de recuperação (*Lessons Learned*)?	Sim	Sim	Sim	Não	Sim
A organização possui um mapeamento da sua cadeia de principais fornecedores?	Sim	Sim	Sim, nível tecnológico.	Não	Sim
A organização possui um mapeamento de conexão de entidades externas (B2B)?	Sim	Sim	Sim	Não	Sim

Fonte: dados coletados em entrevistas realizadas nas instituições

Adicionalmente aos contextos de compilação de informações e análise de dados obtidos nas entrevistas, foi possível avaliar a opinião de especialistas (YIN, 2015) no assunto de risco operacional e continuidade de negócios. A coleta de dados para esta pesquisa envolveu submeter-se às disponibilidades de horário dos entrevistados, sendo que o protocolo aplicado guiado por meio das perguntas previamente estruturadas foi essencial para o planejamento e para condições de abertura para os pontos colocados.

Quanto aos resultados em si, devido à necessidade de globalizar e convergir plataformas tecnológicas, as empresas de capital estrangeiro e multinacionais passam a expor as operações, que estão globalizadas, a problemas de ordem global. A instituição A possui parte da sua operação de contingência de algumas plataformas no México, mais precisamente na cidade do México, que, conhecidamente, possui problemas com a ocorrência de terremotos. De acordo com o *Disaster Recovery Insternational Institute*, há uma análise de risco chamada de TVA ou *Threat Vulnerability Analysis*, que avalia em que o risco da natureza da localidade encontra-se a empresa e quais as chances daquele risco de fato trazer um impacto para o site avaliado. Trata-se de avaliação das disciplinas de gestão de risco operacional e esse ponto foi visto como uma situação de alto risco para esse *site*, que faz o *host* desta operação subir o risco das operações, não só da franquia no Brasil, mas de outros países da América Latina, que fazem parte da estratégia de consolidação informada pelo entrevistado da empresa.

A empresa B passa pelo mesmo problema em relação a riscos de ataques de terrorismo, pois possui parte dos seus sistemas de produção alocados nos Estados Unidos, país que reconhecidamente possui altíssimo risco de ataques dessa natureza. Ainda dentro da análise das instituições A e B, que são bancos de capital estrangeiros, há um dado que deve ser levado em consideração, que são as chamadas plataformas legadas, que são os seus sistemas e plataformas anteriores. Devido a uma necessidade de estar compatível com sistemas que se conectam globalmente, a instituição A, por exemplo, utiliza, em sua operação de tecnologia da informação, plataformas *mainframe*, ou as chamadas plataformas altas, que se conectam à rede por meio de uma placa de rede padrão ethernet que trafega TCP/IP.

O suporte das empresas de prestação de serviço e a mão de obra especializada para manter essa plataforma operativa são de custos altíssimos e não há um contingenciamento total dos módulos que se encontram nessa plataforma, devido a todos os pontos elencados aqui. Já a instituição B possui o mesmo nível de maturidade que a empresa A em todos os aspectos, e, por conseguinte, sua situação se assemelha bastante ao alto nível de resiliência operacional conferido pela análise de seus pontos críticos.

As estratégias de continuidade de negócios estão diretamente focadas na disponibilidade de transações aos processos críticos ao negócio, como no caso das corretoras de seguros e de valores, nos quais os sistemas de transação de liquidação financeira são a prioridade para essas empresas, mas que apresentam determinados pontos de baixa maturidade em seus processos de gestão. Este é o caso das instituições C, D e E, nas quais não há um processo de replicação das plataformas críticas para o site alternativo. Há somente uma replicação de dados com informações em sua natureza de base de dados, assumindo-se, assim, um risco alto no caso da necessidade de uma manobra de recuperação de ambiente *full* produtivo no site alternativo. As empresas multinacionais que foram refletidas nesta pesquisa pelas instituições A e B, por não se considerar suas plataformas de e-mail como missão crítica em seus escritórios principais, assumem que e-mail não é missão crítica em suas franquias no Brasil. Por conseguinte, não estabelecem claramente um plano de recuperação de desastres, ou seja, criam uma dependência de conectividade e com seus *backbones* internacionais operacionais fortíssimos.

Em nenhum dos BIAs avaliados, ficou claro que a plataforma de mensagem era uma aplicação crítica para o negócio, o que é um ponto negativo sob a perspectiva de análise de risco operacional. Mesmo sendo os servidores considerados críticos, apresenta-se que o nível de *hot swap* no contingenciamento é médio. Outro aspecto verificado na análise das informações foi o baixo nível de opção pelos novos "*flavor*s" de tecnologia disponíveis no mercado. Opções como *cloud computing*, ambientes já integrados com aplicações em nuvem, utilizando DevOps ou PaaS, aparecem apenas sendo utilizadas pontualmente, em alguns ambientes das empresas, suportando plataformas de negócios especificas nas instituições B e C. Não há, mesmo por grandes empresas do mercado, uma adoção completa ou em larga escala pela indústria, seja para suportar o ambiente produtivo, seja para suportar o ambiente de contingência desses modelos computacionais e de governança de TI.

As tecnologias de *cloud computing* e a adoção de desenvolvimento de plataformas em nuvem ainda são utilizadas de forma quantitativamente pequenas. Ou seja, são poucas plataformas tecnológicas em que essas opções de estratégia foram utilizadas e, no que tange ao recorte deste estudo, durante o *assessment* realizado com as empresas, nenhuma das opções de computação em rede – ou suas variações – faz parte da estratégia de contingência da empresa.

As empresas A e C possuem um alto grau de estruturação e de maturidade, em termos de governança corporativa, gestão de risco operacional e tecnologia da informação, no que tange a tecnologias legadas e suportam operações críticas ao negócio. Tecnologias legadas são aquelas consideradas como já em processo de decomissionamento, ou em processo de desligamento, pois já alcançaram um nível de obsolescência considerado alto. Esse é o caso dos ambientes de plataforma alta, os chamados *mainframes*. Principalmente nas empresas de grande porte que suportam operações de varejo, há uma dependência alta de plataformas tecnológicas que já entraram em processo de decomissionamento por parte do próprio fornecedor da tecnologia ou do próprio mercado de TI, mas que continuam operando e suportando sistemas críticos de tecnologia de informação. Este é o caso dos bancos que possuem operação de varejo nas empresas A e C, em que os ambientes *mainframes* continuam ativos. Estes ambientes estão conectados à rede TCP/IP das empresas, mas não há um ambiente de contingência duplicado.

O plano de contingência destes ambientes fica por conta de uma reinstalação do ambiente e do *download* de *backup* para a recuperação do ambiente.

Para os aspectos intrínsecos ao processo de aumento de resiliência das atividades operacionais, como processos de gestão de mudança de sistemas críticos de informação, as instituições A e B estão totalmente alinhadas com a as boas práticas. Já a instituição C, possui um processo de gestão de mudança bem estruturado, garantindo que todas as atualizações no *site* de produção sejam replicadas em seus ambientes críticos de informação de contingência, porém isso não ocorre em tempo real. Ou seja, a mudança aplicada ao ambiente de informação – ou plataforma tecnológica – de produção não é refletida de forma sincronizada com os ambientes de contingência.

Sobre a condução dos testes de continuidade, ficou claro que as empresas A e B também possuem alto grau de maturidade na validação dos planos, considerando os tempos de objetivo de recuperação e o direto envolvimento de áreas de negócios, o que estabelece um modelo bastante confiável na validação dos seus planos de contingência e recuperação de desastres. Já a instituição C, possui um processo de validação de seus planos, sendo que o principal ponto crítico de sua operação tecnológica é testado, mas sem uma análise mais aprofundada dos tempos de recuperação, associados a uma validação junto às áreas usuárias. Já as instituições D e E possuem testes de validação de seus planos de recuperação de desastres. No entanto, estas manobras para a instituição D não envolvem as áreas usuárias ou uma validação de um tempo de recuperação (RTO), não conferindo a ela um modelo ideal de validação das manobras de contingência.

No que diz respeito ao mapeamento de suas conexões externas e conexões de negócios (B2B ou B2C), há, nas instituições A e B, um claro mapeamento, envolvendo a análise de seus fornecedores críticos em suas operações de contingência, fazendo com que seja elevado o seu nível de resiliência operacional, incluindo também o envolvimento de alguns destes parceiros em suas manobras de contingência. Estas circunstâncias não estão devidamente refletidas na instituição C, que possui um mapeamento de suas conexões externas e fornecedores. Porém, as validações para fins de planos de contingenciamento ocorrem em um nível tecnológico, considerando as conectividades inerentes ao processo de interligação, mas que não garantem uma operação imediata em caso de acionamento de seus planos, com uma consequente recuperação. Em relação às instituições D e E, estas possuem mapeamentos de seus fornecedores e conexões externas, mas que não estão diretamente refletidas em seus planos de contingência, ou, de alguma forma, sendo validadas durante suas manobras de acionamento de suas estratégias. Há um mapeamento feito e documentado, mas que, para fins de mitigação de riscos em suas operações, possuem um processo ainda considerado de maior risco.

5 CONSIDERAÇÕES FINAIS

O objetivo desta pesquisa foi analisar a capacidade das empresas da indústria financeira em responder a eventos de crises e de total impacto ou indisponibilidade em seus *sites* principais de operação, atendendo aos requisitos específicos da NBR ISO/IEC 22301. Para atingir esse intento, conduzimos entrevistas com os responsáveis pelos setores pertinentes ao assunto em cinco empresas financeiras brasileiras.

Durante as entrevistas conduzidas junto aos profissionais, avaliamos que o grau de maturidade e resiliência frente à possibilidade de incidentes ou eventos com proporções capazes

de impactar as operações delas pode ser considerado médio, para aspectos de governança, políticas, planos e mapeamento de processos de negócio. Nessa avaliação, consideraram-se os aspectos de estruturação de planos de contingência e preparação para possíveis interrupções em suas operações, planejamento estratégico das ações de contingenciamento e análise de impacto ao do negócio.

Essa atividade de ações de contingenciamento (operações e execução de testes integrados com áreas de negócios, fornecedores críticos, conexões externas e a devida gestão de mudança) foi considerada baixa para aspectos intrínsecos às operações dos planos. Nessas operações, são considerados os dados e informações manipulados e incrementados ao longo de suas operações que, em grande parte, ocorrem 24 horas por dia. A relevância da governança de TI, atrelada com a implementação de boas práticas na gestão de continuidade de negócios e no aumento da resiliência operacional, é altíssima e esse foi um dos pontos intrínsecos mais considerados para esta análise. Entre as instituições avaliadas, foi possível observar também um alto grau de similaridades nas estratégias adotadas pelas instituições A, B e C, quanto à gestão de risco operacional e ao grau de maturidade em governança de TI. Assim também ocorre quanto ao valor investido para manter *sites* de contingência, sejam eles ativos da empresa ou locações realizadas com fornecedores externos.

A instituição D, com um porte menor em relação às instituições A, B, C e E, atua com um plano de continuidade de negócios diferenciado, adotando testes de tolerância à falha, enquanto as demais instituições atuam com testes que consideram cenários de total indisponibilidade em seus *sites* principais. Neles, valida-se o RTO, mesmo que em algumas circunstâncias da instituição C isso só se aplique para dados incrementais, significando que somente as empresas A e B executam esse processo de forma total. Notavelmente, apesar de utilizar uma estratégia diferente, o modelo de negócio da própria instituição garante que, mesmo que esta enfrente a possibilidade de um evento crítico, com proporções de impacto alto nas operações, há um risco médio do tempo de resposta ser alcançado de forma adequada para atender as expectativas dos acionistas e dos RTO estabelecidos.

Este estudo demonstrou que a gestão de risco operacional e continuidade de negócios podem ser devidamente associadas com as disciplinas de segurança da informação, que devem ser suportadas por políticas fortes dentro de sua governança corporativa. Portanto, as empresas do setor financeiro, a fim de garantir a própria operação e mitigarem qualquer impacto ao sistema financeiro nacional brasileiro, atuam planejando e testando opções para identificar a melhor estratégia para assegurar a tecnologia e os processos sistêmicos requeridos.

Neste estudo, verificamos que as instituições que operam dentro da janela de operação do sistema financeiro brasileiro, com liquidações financeiras que não atingem a demanda de disponibilidade no regime 24X7, que não contam com a disponibilização de transações *online* realizadas pelos clientes diretamente e que não têm a necessidade de disponibilização de produtos bancários múltiplos a clientes de varejo, requerem um investimento menor para a manutenção de *sites* de contingência. Ainda dentro deste aspecto significativo de apetite ao risco, este estudo tratou da análise de investimento de instituições, como a D, que não mantêm *sites* dedicados associados para contingência das operações, além de aspectos tecnológicos. Seus gestores concluíram que o retorno obtido sobre o investimento em um *site* dedicado não se justifica, devido a ser desnecessário responder a um RTO agressivo, podendo ser realizados outros tipos de manobras junto ao Banco Central Brasileiro, até que as operações mais críticas sejam reestabelecidas. Obviamente, os bancos com modelos de produtos múltiplos com operações no varejo devem realizar outro tipo de estratégia, a fim de garantir a alta disponibilidade de serviços aos clientes.

Desta forma, este estudo também comprovou que o plano de continuidade de negócios deve ser desenvolvido, considerando toda e qualquer individualidade da instituição, de forma a se atentar às reais necessidades da organização, para garantir que as operações tenham a melhor eficiência e o menor dispêndio financeiro. Principalmente, o plano de continuidade visa atender aos processos intrínsecos de uma gestão operacional, testes de contingência integrados com áreas de negócios, fornecedores críticos e conexões externas, visando o alcance dos tempos de recuperação requeridos pela criticidade de negócio.

Como toda pesquisa acadêmica e gerencial, há limitações que envolveram esta pesquisa, como a amostra por conveniência e o tempo de observação das práticas para a constituição do escopo. Também, seria interessante ampliar a amostra de instituições financeiras com outros bancos e outros tipos de serviços, inclusive as atuais *fintechs*. Ainda, futuros estudos podem partir dessas premissas para tirar os vieses de entrevistas apenas com gestores e responsáveis, abordando outros atores e parceiros das instituições.

Este estudo não almejou finalizar as discussões acerca da continuidade de negócios e obediência às regras e normas de melhores práticas da GC em empresas financeiras brasileiras. Pelo contrário, a intenção primeira foi contribuir com as informações sobre esses construtos para o setor e para a academia.

6 REFERÊNCIAS

ABNT - http://www.abnt.org.br/, acesso em 18/07/2019.

ABNT - Associação Brasileira De Normas Técnicas. Gestão da qualidade – Diretrizes para a qualidade no gerenciamento de projetos - NBR ISO 10006. **Rio de Janeiro**, 2000. 18p.

ABNT - Associação Brasileira De Normas Técnicas. NBR 15.999. 1*:* Gestão de continuidade de negócios parte 1: Código de prática. **São Paulo**, 2007.

ABNT - Associação Brasileira De Normas Técnicas. NBR ISO 22301. 1: Segurança da Sociedade – Sistema de Gestão de continuidade de negócios – Requisitos. **São Paulo**, 2013.

ALEVATE, William. **Gestão da continuidade de negócios**. Elsevier Brasil, 2014.

BACEN - Banco Central do Brasil. Resolução 3.830. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em: http://www.bcb.gov.br/pt-br. Acesso em 26 set. 2015.

BARDIN, Laurence. **Análise de Conteúdo**. Lisboa: Edições 70. 1977.

BEAL, Daniel J. ESM 2.0: State of the art and future potential of experience sampling methods in organizational research. **Annu. Rev. Organ. Psychol. Organ. Behav.**, v. 2, n. 1, p. 383-407, 2015.

BRITISH STANDARDS, I. Business continuity management. Part 1, Code of practice. **London, British Standards**. 2006.

CHAVEZ-DEMOULIN, Valérie; EMBRECHTS, Paul; HOFERT, Marius. An extreme value approach for modeling operational risk losses depending on covariates. **Journal of Risk and Insurance**, v. 83, n. 3, p. 735-776, 2016.

COOPER, Donald R.; SCHINDLER, Pamela S. **Métodos de Pesquisa em Administração-12ª Edição**. McGraw Hill Brasil, 2016.

COSO – **Committee of Sponsoring Organizations of the Treadway Comission** et al. COSO gerenciamento de riscos corporativos - estrutura integrada: sumário executivo. **Recuperado em**, v. 26, 2011.

CUI, Tingru et al. Information technology and open innovation: A strategic alignment perspective. **Information & Management**, v. 52, n. 3, p. 348-358, 2015.

CVM. Comissão de Valores Mobiliários - Recomendações da CVM sobre Governança Corporativa**. São Paulo**, 2002.

DE ABREU CAMPANÁRIO, Milton et al. Governança corporativa em empresas públicas. **Race: revista de administração, contabilidade e economia**, v. 13, n. 2, p. 689-718, 2014.

ECONOMATICA – https://economatica.com/ - **Relatório de sistema de investidores** disponibilizado e acessado em agosto de 2016.

EISENHARDT, K.; PIEZUNKA, Henning. Complexity theory and corporate strategy. **The SAGE handbook of complexity and management**, p. 506-523, 2011

FAGUNDES, E. M. *Cobit* – **Um kit de ferramentas para gestão de TI**. Acessado em: 06/09/2016 em: http://efagundes.com/artigos/cobit, 2012.

FEBRABAN – Federação Brasileira dos Bancos- https://issuu.com/revistaciab/docs/revista_ciab_61_fev16 último acesso em agosto de 2019.

IBGC, Instituto Brasileiro de Governança Corporativa. **Código de Melhores Práticas de Governança Corporativa.** 2009.

HERMALIN, Benjamin E. Transparency and corporate governance. In: **Enterprise Law**. Edward Elgar Publishing, 2014.

LIU, Xiang; ZHANG, Chen. Corporate governance, social responsibility information disclosure, and enterprise value in China. **Journal of Cleaner Production**, v. 142, p. 1075-1084, 2017.

LUNARDI, Guilherme Lerch et al. Governança de TI no Brasil: uma análise dos mecanismos mais difundidos entre as empresas nacionais. **Simpósio de Excelência em Gestão e Tecnologia (4.: 2007 out.: Resende). Anais do SEGeT. Resende: Associação Educacional Dom Bosco, 2007.**, 2007.

MCCAHERY, Joseph A.; SAUTNER, Zacharias; STARKS, Laura T. Behind the scenes: The corporate governance preferences of institutional investors. **The Journal of Finance**, v. 71, n. 6, p. 2905-2932, 2016.

MECKLING, Jonas. Oppose, support, or hedge? Distributional effects, regulatory pressure, and business strategy in environmental politics. **Global Environmental Politics**, v. 15, n. 2, p. 19-37, 2015.

MILES, Samantha. Stakeholder theory classification: A theoretical and empirical evaluation of definitions. **Journal of Business Ethics**, v. 142, n. 3, p. 437-459, 2017.

OLIVEIRA, Oderlene; FORTE, Sérgio. A indústria bancária brasileira: Construindo cenários prospectivos e identificando as estratégias de utilização mais provável. **Revista de Gestão dos Países de Língua Portuguesa**, v. 8, n. 2, p. 64-77, 2009.

PEDOTE, Cristiane de Freitas Salto. **Análise e gerenciamento de risco: Gestão do risco operacional em instituições financeiras**. 2002. Tese de Doutorado.

PEREIRA, Luciano de Castro. **O risco operacional em instituições financeiras e a influência de fatores do ambiente externo**, 2004.

PORTER, Michael E. & MONTGOMERY, Chyntia. *Estratégia: a busca da vantagem competitivas.* Rio de Janeiro: Ed. Campus, 1998.

RIBEIRO, Henrique César Melo et al. Entender para progredir: análise da pesquisa em governança corporativa no Brasil. **Gestão Contemporânea**, n. 12, 2012.STEINBERG, Richard M. **Governance, Risk Management, and Compliance: It Can't Happen to Us--Avoiding Corporate Disaster While Driving Success**. John Wiley & Sons, 2011.

TRICKER, RI Bob; TRICKER, Robert Ian. **Corporate governance: Principles, policies, and practices**. Oxford University Press, USA, 2015.WANG, Dong-hua; XU, Chi. Operational risk measures for banks based on nonparametric methods. **Journal of Management Sciences in China**, n. 3, p. 9, 2015.

WALLACE, Michael; WEBBER, Lawrence. **The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets**. Amacom, 2017.

YIN, Robert K. **Estudo de Caso-: Planejamento e métodos**. Bookman editora, 2015.