

A importância da governança corporativa para o processo de aquisição de equipamentos de TI

Corporate governance importance for the acquisition process of IT equipments

Rogério de Campos¹

Renata Carolina Grotta²

José Donizette Basileu³

Amanda dos Santos Costa Soares⁴

Recebido: 16/10/2016

Aprovado: 30/11/2016

Publicado: 15/12/2016

Processo de Avaliação: Double Blind Review

RESUMO

Neste estudo são abordadas as etapas que ocorreram no processo de aquisição de equipamentos de informática de alto valor agregado, bem como as ações que foram empreendidas para o desdobramento do processo de aquisição. Assim, por meio de estudo de caso único de uma empresa do ramo educacional, foi analisada a importância da gestão para a resolução de conflitos de interesses no processo de aquisição, incluindo as fases que ocorreram nesse processo, do seu início até a sua finalização, para a compra dos equipamentos de TI. O relato descreve as etapas que envolveram as dificuldades de funcionamento de TI em setores essenciais da empresa, quando serão especificados os riscos que deixaram a empresa vulnerável por um determinado tempo.

1Cursando mestrado Profissional em Administração e Governança Corporativa no Centro Universitário das Faculdades Metropolitanas Unidas, Pós-graduado em Logística Empresarial e em Rede de Computadores, Graduado em Sistemas de Informação. E-mail: info.rcampos@gmail.com

2 Cursando mestrado Profissional em Administração e Governança Corporativa no Centro Universitário das Faculdades Metropolitanas Unidas, Especialista em Administração de Serviços e Graduada em Administração Hoteleira. E-mail: renata.grotta@gmail.com

3 Cursando mestrado Profissional em Administração e Governança Corporativa no Centro Universitário das Faculdades Metropolitanas Unidas. E-mail: jdbasileu@gmail.com

4 Cursando Graduação da FMU em Administração de Empresas. E-mail: amanda.costa.adsc@gmail.com

Nas ações realizadas no processo de aquisição, houve a necessidade de realização de melhor justificativa, com base a metodologia de Gestão de Riscos, para identificar os processos críticos voltados para os clientes da empresa. Para a conclusão do processo de aquisição, foi abordada a necessidade do envolvimento da Governança Corporativa da empresa, para buscar uma solução adequada no conflito de interesses, para evitar prejuízos para a empresa e garantir a sobrevivência da organização. **Palavras-chave:** Gestão de Risco; Gestão de Continuidade de Negócios; Governança Corporativa.

ABSTRACT

This study will address the steps that occurred in the process of acquiring high-value computer equipment, as well as the actions that were taken to the split of the procurement process. Thus, by means of a single case study of a company's educational branch, will be analyzed the importance of management to resolve conflicts of interest in the procurement process, including the phases that occurred in the process of its inception to its completion, for the purchase of IT equipment. The report will describe the steps that involved the difficulties of IT operation in essential sectors of the company, when the risks left the company vulnerable for a certain time will be specified. The actions carried out in the procurement process, there was the need to perform better justification based Risk Management methodology to identify critical processes focused on the company's customers. For the completion of the acquisition process, the need for the involvement of Corporate Governance of the company will be approached to seek an appropriate solution to the conflict of interests to avoid damage to the company and to ensure the survival of the organization.

KEYWORDS: Risk Management; Business Continuity Management; Corporate Governance.

INTRODUÇÃO

No cenário atual, as empresas necessitam estar em constante atualização tecnológica, buscando executar melhorias no seu parque tecnológico, envolvendo as necessidades do negócio com a compatibilidade para a execução de processos essenciais. Assim, torna-se necessário interferir no desempenho de operações sem trazer prejuízos para o funcionamento do negócio. É nesse sentido que torna-se comum, mesmo em tempos de crise, alocar investimentos em Tecnologia da informação - TI, para garantir que a infraestrutura traga resultados positivos para as empresas.

Este tema se posiciona como relevante para as organizações, que necessitam trabalhar suas operações de modo preventivo, uma vez que, atualmente, grande parte

das empresas desenvolvem suas atividades de modo corretivo, ou seja, só buscam a solução quando algo não funciona, e, como consequência, têm vários riscos relacionados aos problemas de TI como: falhas na implantação de novos sistemas, diminuição de capacidade operacional e interrupções no funcionamento de equipamentos essenciais de TI, que podem comprometer o funcionamento do negócio.

De acordo com Assi (2012), entende-se que o risco é algo que pode não dar certo e envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às perdas ou ganhos, advindos de acontecimentos não planejados. Assim, é importante que as empresas realizem investimentos em equipamentos de infraestrutura de TI, conforme o seu modelo de classificação de ativos, de acordo com os possíveis riscos para o negócio, para garantir atualização do parque tecnológico, a fim de mitigar futuros problemas.

Desta maneira, é importante o desenvolvimento da análise dos processos críticos da empresa com base na gestão de riscos, para a identificação das ameaças e vulnerabilidades. Segundo Silva, Gomez e Miranda (2013), o gerenciamento de continuidade de serviços de TI, como parte do gerenciamento de continuidade de negócios ligada à análise de risco, em que são classificadas as ameaças e as vulnerabilidades do negócio e da TI, tem objetivo de reduzir a possibilidade de um risco se tornar um problema a ser concretizado.

No estudo de Assi (2012), o risco pode envolver uma ou mais variáveis com potencial de causar dano ao patrimônio das empresas, e aos processos que acompanham a estrutura de bens tangíveis e intangíveis. Como os riscos são inerentes ao negócio, a gestão de riscos trata da identificação das ameaças que podem afetar o negócio. Sendo assim, um componente crítico das atividades de uma organização é a identificação de riscos, uma vez que é importante se considerar a subjetividade inerente ao risco ocorrer ou não. Logo, os riscos permeiam em todas as empresas, assim como nas atividades que são realizadas, inclusive o não investimento em tecnologia. Os riscos podem possuir diversas formas e podem ser caracterizados como: físico, estrutural, econômico, social e ambiental, desdobrando-se em diversos componentes e em sucessivos em vários níveis de detalhamento (Guimarães, 2006).

É nesse contexto que o objetivo do estudo é descrever as etapas do projeto de aquisição de equipamentos de informática. A pesquisa desenvolvida aborda os potenciais impactos advindos de uma reprovação de aquisição, que pode trazer resultados negativos no processo de ensino e na gestão administrativa de atividades, que dependem do uso da TI para garantir o funcionamento de atividades relevantes para o negócio.

Assim, com base na implantação da gestão de riscos e a gestão da continuidade do negócio - GCN, a empresa buscou mitigar ao máximo os impactos que poderiam ser gerados aos clientes envolvidos nos processos essenciais da empresa.

REFERENCIAL TEÓRICO

A gestão de riscos deve ser realizada em todas as atividades de uma organização, principalmente quando a mesma depende exclusivamente do acesso aos recursos de TI. Andrade et al. (2011) definem que, independente do porte da empresa, é necessário um sistema de informação para o sucesso e funcionamento para a sobrevivência das organizações, uma vez que os sistemas contribuem com a qualidade do atendimento, da entrega do produto e prestação do serviços.

Os riscos operacionais relacionam-se às eventuais perdas advindas de um gerenciamento inadequado de sistemas, ou até mesmo de uma administração que não seja adequada (Jorion, 1997).

Logo, a elaboração do plano voltado a riscos deve fazer parte da cultura organizacional, para que os serviços sejam restabelecidos em caso de paralisação nos sistemas de informação, com a elaboração de planos e testes para mitigar ao máximo o impacto da concretização de um risco (Silva et al., 2011).

É nesse sentido que é necessário estar preparado para agir em situações e crises inesperadas de forma organizada, estruturada e mitigando potenciais perdas aos negócios. Essa é o principal papel da governança e gestão de riscos e continuidade de negócios (Brito, 2010).

De acordo com Andrade et al. (2011), o plano de continuidade operacional e recuperação de desastre perfazem o plano de contingência, tratando os riscos de um sistema de informação ficar indisponível, preservando assim a qualidade dos negócios ou do serviço prestado.

Sendo assim, a Gestão de Continuidade de Negócio trata sobre como fazer com que a quantidade mínima de serviços continue operando, enquanto prepara-se a recuperação do negócio (Silva, Gomez e Miranda, 2013).

Segundo Assi (2012), a existência de riscos associados à perda ou interrupção longa dos serviços da organização representa preocupação estratégica com o negócio e com a

imagem da organização. Sendo que tais problemas podem causar sérias dificuldades e até prejudicar a habilidade da organização em conduzir suas atividades de negócios. Para os riscos em potenciais, têm-se o estabelecimento de planos de contingência e de recuperação.

É nesse sentido que o estudo de Silveira (2010) aponta que, a limitação técnica dos tomadores de decisão é um problema a ser mitigado pelos mecanismos de governança, quando as decisões podem em algum momento serem concentradas por pessoa que não possui o conhecimento técnico necessário para as decisões-chave de uma companhia, como um investimento.

Nesse contexto, a governança corporativa trata sobre os problemas de agência, que surgem com a separação de papéis que existem entre propriedade (principal) e controle (agentes), devido às diferenças de motivação e objetivos, assimetria de informação e preferências de risco que existem entre os proprietários e os agentes (Jensen e Meckling, 1976). Segundo os mesmos autores, as agentes podem agir em benefício próprio, e não segundo os benefícios da empresa, dos acionistas e demais partes interessadas, gerando conflitos de interesse. Para dirimir os problemas de agência, as organizações e seus acionistas devem praticar algumas medidas para alinhar interesses dos envolvidos, objetivando o sucesso da organização. Para isso, devem ser propostas medidas que incluem práticas de monitoramento, controle e ampla divulgação de informações.

METODOLOGIA

A pesquisa desenvolvida se classifica como pesquisa qualitativa empregando a técnica de estudo de caso único. A opção metodológica adotada estabelece relação com a abordagem de Richardson *et al.* (1999), que aponta a adequação do uso de pesquisa qualitativa nas investigações destinadas a compreensão da complexidade de um problema, a analisar o relacionamento de variáveis, a classificar e analisar processos dinâmicos. Para Yin (2010) o estudo de caso se configura como uma investigação adequada para o entendimento de fenômenos complexos.

A pesquisa apoiou-se na identificação de dados que viabilizassem ao final do estudo responder ao objetivo da pesquisa. Para o atendimento desta meta, utilizou-se duas diferentes fontes de informações, a saber: i) entrevistar funcionário da instituição

objeto de pesquisa que estava envolvido no processo de aquisição de equipamentos de informática; ii) coleta de dados documentais internos a empresa investigada.

A instituição objeto foi analisada por membro da equipe de TI que participou do processo de aquisição e que possibilitou relatar o desenvolvimento dessa pesquisa. Vale ressaltar que esses fatos atualmente são vivenciados por outras empresas que dependem de base de metodologias para garantir aprovação de projetos com base em questões técnicas e dos impactos ao negócio.

O estudo se desenvolveu com o auxílio de um roteiro elaborado a partir dos objetivos da pesquisa, da revisão teórica e informações do processo de aquisição da empresa, sendo caracterizado como um relato tecnológico, comum aos programas de mestrado profissional, assim optou-se por apresentar e analisar as informações em um texto conciso, que incorpora de forma indistinta os dados da investigação documental.

A pesquisa se desenvolveu em empresa do ramo educacional, atuante tanto no ensino básico e médio, quanto no universitário e pós-graduação. A Instituição de ensino objeto de pesquisa possui três unidades físicas na cidade de São Paulo. O início das suas atividades foi no ano de 1952, período este em que havia baixa oferta de instituições de ensino superior. No entanto, as atividades voltadas ao ensino se iniciaram em período anterior, mais precisamente no ano de 1870, quando um casal de missionários abriu uma escola voltada ao ensino básico. As atividades em ensino superior se iniciaram em 1885, com a oferta do curso de Filosofia, em 1890, o curso de Comércio, e em 1896, com os cursos de Engenharia. Tal trajetória posiciona a instituição como uma das pioneiras no ensino superior.

A Instituição objeto de pesquisa possui como premissas a qualidade de ensino e a oferta de metodologias e recursos inovadores para seus alunos. Nesse sentido, a Instituição, para garantir a sua infraestrutura de ensino em perfeito funcionamento, procura estar em constante desenvolvimento com atualizações dos equipamentos. Frente ao propósito de atualização de seus equipamentos de informática, a Instituição iniciou pesquisas de viabilidade técnica e financeira, ficando a cargo do departamento de Tecnologia da Informação identificar os futuros problemas que poderiam ocorrer e determinar qual a melhor opção tecnológica disponível no mercado. Determinou-se também que o departamento de informática deveria incluir estes custos no seu budget de investimento. O projeto de atualização dos equipamentos se enquadrou dentro do contexto educacional e administrativo como elemento importante para o funcionamento de suas operações aos clientes.

O processo de análise e viabilidade de aquisição dos equipamentos envolveu o levantamento das necessidades de várias áreas da empresa. Dentre as áreas se destacam a de Tecnologia da Informação, Gerência Administrativa, Recursos Humanos, Financeiro e toda área educacional, incluindo diretoria, coordenações, os laboratórios de informática, as bibliotecas e secretarias. Foi desenvolvida análise das características técnicas necessárias para equipamentos pela área de TI, que faz a análise e o detalhamento do projeto frente às opções apresentadas pelo mercado.

O parque tecnológico de equipamentos da instituição contava com aproximadamente 500 computadores na filial estudada, sendo que, somente os laboratórios continham 175 micros, para um total de 3000 alunos do colégio e da universidade divididos no período manhã, tarde e noite. A proposta do projeto de equipamentos envolvia a aquisição de 15 *switches* da marca DELL para melhorias na infraestrutura de redes de computadores do Campus, com o objetivo de garantir o funcionamento dos sistemas de informação, tecnologia Wi-Fi para equipamentos móveis e dos computadores: dos laboratórios de informática, funcionários das áreas educacional e administrativa. Os equipamentos de redes do processo de aquisição seriam adquiridos para substituição dos equipamentos obsoletos tecnologicamente, com base em constantes travamentos e velocidade baixa para a comunicação em rede. Vale destacar que estas variáveis se materializavam no fator preponderante do processo de renovação dos equipamentos, pois eram objeto de estudo do departamento de TI que havia detectado tal necessidade. E, adicionalmente, para evitar problemas de funcionamento da rede de computadores para os usuários.

No sistema de chamados do *Help Desk* - local onde é realizado a centralização de todos os chamados técnicos de problemas dos usuários, foi possível perceber o aumento na quantidade de chamados, sendo que a maioria dos chamados envolviam os equipamentos de redes que geravam problemas no funcionamento dos sistemas da empresa.

O projeto de aquisição envolveu uma força tarefa que, com base em estudo de riscos, identificou a necessidade de investimentos, a curto prazo, em equipamentos novos, que pudessem garantir o funcionamento, evitando os travamentos dos equipamentos de redes, impactando, principalmente, em problemas para os sistemas que eram utilizados pelos usuários das áreas: administrativa e educacional. Por outro lado, os alunos como clientes principais da empresa tinham a necessidade de utilizar a internet durante as aulas, uma vez que grande parte de todo o conteúdo de aulas e

atividades eram disponibilizados no sistema MOODLE, bem como em serviços para os alunos como: Bibliotecas, Laboratórios, Secretarias e Financeiro.

Outra demanda do setor de informática era a necessidade de disponibilizar acessos a rede sem fio para os alunos e professores em todo o campus, por meio de *smartphones*, *notebooks* e *tablets*, para uso via rede sem fio nas bibliotecas, salas de aula e outros ambientes destinados a pesquisas, de acordo com a política de acesso a internet desenvolvida pela área de segurança da informação.

3. ANÁLISE E DISCUSSÃO DOS DADOS

No estudo realizado na instituição, foi verificado que a empresa tinha um parque tecnológico em TI funcionando no seu limite em relação as suas operações, e isso poderia, em algum momento, gerar problemas para empresa por ocasião de alguma falha em equipamentos de TI. O parque tecnológico tinha limitações quanto à quantidade de equipamentos de redes, os *switches*, que tinham como papel principal em garantir o funcionamento da rede de computadores da empresa, na qual era o meio pelo qual os usuários se comunicavam com os servidores principais e secundários, de acordo com a estrutura de rede Cliente-Servidor.

Os *switches* utilizados para garantir processos principais do negócio estavam com mais de 8 (oito) anos de vida, condição esta que potencializava a possibilidade de ocorrências de constantes problemas e falhas para o funcionamento dos sistemas da empresa. Qualquer equipamento de rede que gerasse falha, poderia comprometer a estrutura da empresa gerando impacto em vários usuários e departamentos que dependiam dos equipamentos de rede funcionamento normal de atividades.

O Departamento de TI, depois de ter realizado análise e classificação dos seus ativos críticos, conseguiu detectar o crescimento do uso da TI por necessidade em demanda dos usuários do Campus. Sendo assim, foi considerada necessária a expansão do parque tecnológico, por conta de instalações de novos equipamentos como: câmeras de monitoração para o Centro de Controle Operacional, pontos de redes do WI-FI e pontos de rede para cobrir as necessidades de usuários novas instalações da empresa.

De acordo com o modelo de negócio dessa filial, foram priorizados os atendimentos aos alunos para os serviços de Laboratórios de Informática, Departamento Financeiro,

Secretarias e Bibliotecas, mas os departamentos envolvidos dependiam exclusivamente dos recursos de TI, principalmente do acesso ao Sistema da empresa. Assim, tornou-se necessário a criação de um modelo que pudesse contemplar a Gestão de Continuidade do Negócio - GCN, para evitar interrupções decorrentes por falhas em equipamentos de TI, ou ainda pela ausência de equipamentos para cobrir os planos de contingências. Para Silva (2013), a gestão de continuidade do negócio permite que, em caso de desastres, os serviços de TI sejam restaurados, conforme o tempo combinado de nível de serviço.

Com base na necessidade de funcionamento de processos críticos, o departamento de TI dependia da aprovação dos equipamentos de redes a curto prazo, para dimensionar os locais críticos do parque tecnológico, e assim garantir o funcionamento da estrutura e alocação novos pontos de redes no Campus para cobrir a Gestão da Continuidade do Negócio.

Seguindo as etapas do processo, com objetivo de aprovação do processo de aquisição, a empresa desenvolveu as justificativas no modelo do GCN - Gestão da continuidade do negócio, ligado a gestão de riscos, que serve de modelo para as empresas em garantir que processos empresariais não possam parar, principalmente a possibilidade dos riscos operacionais das empresas. No estudo de Silva, Gomez e Miranda (2013), a GCN está ligada a fazer com que a quantidade mínima de serviços continue operando, enquanto se prepara a recuperação do negócio. De acordo com Andrade et al. (2011), o plano de continuidade operacional e recuperação de desastre perfazem o plano de contingência tratando os riscos de um sistema de informação ficar disponível, preservando assim a qualidade dos negócios ou do serviço prestado.

Nesse sentido, foi elaborado o projeto de aquisição de novos equipamentos, tendo sido anexado as justificativas iniciais que demonstravam atualização dos equipamentos de redes obsoletos, para garantir a infraestrutura para suprir o funcionamento de processos essenciais do campus de acordo com o GCN. O processo de compra foi encaminhado para aprovação para o Gestor de TI e Gerente Administrativo, que atuavam com poderes para aprovação de projetos de melhorias para a Gestão de TI dessa filial. Na sequência, foi submetido aos Diretores e ao CEO (diretor presidente) que estavam alocados na Matriz da empresa. Vale lembrar que nesse período, de acordo com o processo de aprovação, o Departamento de TI possuía orçamento anual aprovado pelos Gestores para realizar a compra dos equipamentos citados nesse estudo, ou seja, havia verba disponível no centro de custo do departamento de TI para aquisição dos equipamentos novos de redes.

Assim sendo, foram realizados os contatos com três empresas conceituadas no mercado de TI, que com base nos requisitos da empresa, encaminharam os seus orçamentos e cotações de preços em moeda dólar para análise da Instituição.

No processo de aquisição, a maioria dos gestores e diretores efetivaram as aprovações no sistema integrado ERP no módulo de compras. No entanto, por questões de conflito de interesses, o processo de aquisição parou por falta de aprovação do Diretor Financeiro (CFO), que não aprovou o investimento por não conhecer tecnicamente o uso dos equipamentos para essa filial, que foram elaboradas conforme o modelo do GCN, que apontava a descrição de futuros problemas que poderiam ocorrer em atividades principais da empresa. O Diretor Financeiro (CFO) não aprovou a aquisição considerando apenas os valores a serem depreendidos para o investimento. O estudo de Silveira (2010) aponta que, a limitação técnica dos tomadores de decisão é um problema a ser mitigado pelos mecanismos de governança, quando as decisões podem em algum momento serem concentradas por pessoa que não possui o conhecimento técnico necessário para as decisões-chave de uma companhia, como um investimento.

Jensen e Meckling (1976) destacaram que os problemas de agência surgem com a separação de papéis que existem entre propriedade (principal) e controle (agentes), devido às diferenças de motivação e objetivos, assimetria de informação e preferências de risco que existem entre os proprietários e os agentes. Segundo os autores, as agentes podem agir em benefício próprio, e não segundo os benefícios da empresa, dos acionistas e demais partes interessadas, gerando conflitos de interesse. Para diminuir o problema de agência, as empresas e seus acionistas deveriam praticar algumas medidas para alinhar interesses dos envolvidos, objetivando o êxito da organização. Para isso, foram propostas medidas que incluíam práticas de monitoramento, controle e ampla divulgação de informações. A este conjunto de medidas estipulou-se chamar de Governança Corporativa.

Assim, como o projeto não foi aprovado neste primeiro momento, o departamento de Tecnologia da Informação foi comunicado, tendo que fazer novas justificativas, incorporando a elaboração da gestão de riscos que identificava os possíveis riscos para o negócio pela falta dos novos equipamentos de infraestrutura, para garantir o funcionamento de recursos essenciais da empresa.

A empresa, por meio da equipe de TI, elaborou a gestão de riscos para identificar futuros problemas para a estrutura da empresa. Assim, de acordo com Assi (2012), o risco tem a principal característica de probabilidade de ocorrer ou não, conforme

escolha e ação dos gestores, os riscos podem ser interpretados como sendo ameaças ao alcance dos objetivos organizacionais.

Assim, a gestão do risco é definida como um conjunto de processos que possibilitem a identificação e implantação de medidas de proteção, para dirimir os riscos que podem ocorrer com os ativos de informação das empresas, e equilibrá-los com os custos operacionais e financeiros (Beal, 2005).

Algumas categorias de riscos, às quais as organizações empresariais podem estar sujeitas, estão relacionadas ao risco operacional. A identificação, de forma estruturada, dessas categorias, permite minimizar a probabilidade de ter perdas derivadas de desastres e crises operacionais, provendo ferramentas para ações em momentos de crise (Hoffman, 2002; Shea, 2006).

No segundo momento, novas justificativas para aprovação foram incluídas a importância dos equipamentos de redes como: os *Switches*, que tinham a função básica de trazer a conectividade entre os computadores, bem como permitir a estabilidade da infraestrutura de redes da empresa. O equipamento de rede significava o recurso de TI essencial para a comunicação de dados para gerar integração e conectividade, a fim de garantir o funcionamento de acesso aos sistemas e da internet para uso dos usuários.

O Departamento de Tecnologia da Informação justificou as necessidades a Governança Corporativa para adquirir os novos equipamentos, a fim de garantir o funcionamento de infraestrutura da empresa, com base possíveis problemas de operações que poderiam ocorrer na empresa, no qual foi constatado que se algum equipamento viesse a parar de funcionar, o mesmo poderia comprometer diretamente os processos críticos, conforme identificados no Quadro 1 a seguir:

Quadro 1 - Problemas eventuais das áreas da empresa

Área	Problema	Impacto
Laboratórios de Informática	Sem acesso a internet	Alunos e professores
Secretarias	Falta de atendimento	Alunos
Bibliotecas	Sem acesso para empréstimo de livros e pesquisas na internet	Alunos
Financeira	Sem acesso aos acordos financeiros e pagamento de boletos	Alunos e fornecedores
Recursos Humanos	Sem acesso ao sistema de folha de pagamento	Funcionários
Tecnologia da Informação	Sem acesso a internet e aos servidores	Todos os usuários

Fonte: Elaborado pelos autores (2016).

Os equipamentos de redes em referência desse estudo são especificados no Quadro 2, assim como, seguem informados os principais impactos para o negócio que foram identificados.

Quadro 2 - Quadro de riscos e impactos do equipamento de rede para o negócio

Caso	Risco do Equipamento na Rede	Impacto
A	Travamento por excesso de carga na rede	Baixo
B	Perda de configuração após queda de energia	Médio
C	Queima do equipamento após incidente	Alto

Fonte: Elaborado pelos autores (2016).

Para todos os casos acima foram considerados a categoria de riscos para os equipamentos de rede obsoletos do estudo, que a empresa possuía no seu parque tecnológico, e dependendo do tipo de incidente (falha), seria acionado rapidamente um plano de ação para conter o risco, para evitar impacto a estrutura da empresa. Nos três casos apresentados, a empresa estaria vulnerável, pois todas param as atividades da empresa em alguma situação, mesmo considerando o caso de baixo de impacto. Assim, se torna necessário entender os casos apresentados de maneira a buscar melhorias para garantir a Gestão da Continuidade do Negócio.

No caso do risco A, se o *switch* viesse a travar após queda de energia, o mesmo teria um nível baixo de risco para o negócio. O equipamento seria reiniciado pela equipe de TI, voltando a funcionar em média em até 30 minutos após a sincronização com os outros equipamentos interligados em rede. Assim, o problema seria solucionado nesse tempo, mas muitos usuários interligados a esses equipamentos de rede não teriam acesso aos recursos de TI no tempo determinado para a recuperação dos serviços.

No caso do risco B, o nível de risco seria médio para o negócio. O tempo para resolução seria mais alto, em média de 2 horas, podendo variar dependendo do caso até 5 horas para a reconfiguração dos equipamentos de rede, sendo que os usuários ficariam parados aguardando o retorno dos serviços de TI nesse tempo.

No caso do risco C, não seria possível executar o plano de ação, portanto, a Gestão de riscos considerou esse como crítico para a estrutura da empresa, pois o Departamento de TI não teria outros equipamentos disponíveis para utilizar como contingência, para trocar o equipamento queimado. Assim, nesse caso, as atividades da empresa seriam todas impactadas, e poderiam gerar problemas para o negócio por falta de comunicação com os sistemas integrados da empresa.

Vale ressaltar que os casos A e B aconteciam com frequências na empresa, pelo fato de serem equipamentos obsoletos e por ocorrer muitas quedas de energia, portanto, tinham a necessidade de muitas manutenções periódicas. Para o risco C, que está ligado diretamente ao *Rack* central, ou seja no *Data Center* da empresa, o impacto seria bem maior para todos os usuários da empresa, podendo ocorrer a intervenção de vários dias sem acesso a rede e sistemas na empresa. Estes fatos que são confirmados por Assi (2012), que afirma que os sistemas eletrônicos de informação apresentam riscos que devem ser efetivamente controlados, para evitar interrupções dos serviços e prejuízos em potencial. Para isso, sempre se propõem planos de contingência, que permitam à organização operar independentemente dos problemas ocorridos.

No âmbito da gestão da empresa, conforme as boas práticas de Governança Corporativa, Rosseti e Andrade (2014) afirmam que os administradores de todas as áreas corporativas são representantes dos proprietários, e suas decisões devem estar voltadas para formular e implementar planos estratégicos e políticas operacionais que maximizem o retorno dos investimentos.

As boas práticas de governança corporativa, com seus mecanismos de controle, auxiliam as organizações para a verificação de que os planos estratégicos estão sendo executados pelos diretores (IBGC, 2015).

Dessa maneira, a empresa ficou desprotegida por não considerar os investimentos em TI como algo importante para o negócio.

O processo de aquisição envolveu um estudo minucioso que foi identificado com base na elaboração da gestão de riscos para o funcionamento do negócio. Nesse contexto, se adicionou as vulnerabilidades dos ativos da empresa, ou seja, tudo aquilo que pudesse impactar em ameaças para o negócio, que foram realizados com base no plano de respostas aos riscos que envolvia eventuais riscos para um determinado ativo.

Com base no estudo desenvolvido pela equipe de TI, com a relação aos possíveis riscos enfrentados pela empresa, constatou-se a necessidade de efetivação dos investimentos para evitar problemas na infraestrutura e para diminuir o número de chamados dos usuários ao *Help Desk*. Enfim, a empresa ficou vulnerável por 2 (dois) anos, com poucas possibilidades para o controle das operações em caso de falhas. Segundo Assi (2012), a existência de riscos associados à perda ou interrupção longa dos serviços da organização representa preocupação estratégica com o negócio e com a imagem da organização. Sendo que tais problemas podem causar sérias dificuldades e até prejudicar a habilidade da organização em conduzir suas atividades de negócios.

Para os riscos em potenciais, têm-se o estabelecimento de planos de contingência e de recuperação.

Em outro momento, conforme nova justificativa, por meio do modelo de Gestão de riscos, o processo de aquisição foi submetido novamente para aprovação ao alto escalão da empresa que, por intermédio do Gerente Administrativo dessa filial, justificou a necessidade detalhada dessa filial. Novamente foi submetido para aprovação do processo de aquisição aos Gestores diretos, CIO, CEO, Diretores e o membro do conselho de administração da empresa.

Com o encaminhamento de novas justificativas de acordo com a gestão de riscos, foi constatado que a falta de investimentos em TI poderiam causar prejuízos para a empresa, assim o Diretor financeiro (CFO), entendendo as novas justificativas e considerando os problemas que poderiam ser causados para a infraestrutura de TI dessa filial, avaliou o impacto para o negócio, efetivando aprovação do processo de aquisição dos recursos de TI.

O processo foi concluído com as aprovações de todas as partes envolvidas com a Governança Corporativa, sem a ocorrência de novos questionamentos. O processo de aquisição foi aprovado no tempo de aproximadamente de [2 (dois) anos de negociação com a gestão, e nesse tempo a empresa ficou vulnerável aos riscos. Vale ressaltar que muitos dos problemas de usuários foram relatados no sistema de chamados do *Help Desk*, que teve aumento devido as ocorrências de muitas paradas nos sistemas, subindo a insatisfações e reclamações por parte de usuários do sistema, bem como dos clientes que dependiam do acesso aos recursos de TI.

CONSIDERAÇÕES FINAIS

Esse relato mostra a importância em identificar os riscos que a empresa está sujeita, com profissionais qualificados e envolvidos na elaboração de projetos, que possam identificar os riscos que estejam relacionados com os ativos críticos da empresa, bem como adotar medidas preventivas para corrigir os futuros problemas operacionais.

O processo de aquisição de equipamentos de alto valor agregado teve êxito, pela perspectiva da Governança Corporativa, que entendeu o conflito de agência, agiu no tempo certo, para impedimento de problemas que pudessem causar dificuldades no

funcionamento das atividades da filial da instituição, baseados no planejamento realizado pelo Departamento de TI.

Podemos considerar nesse estudo que a Governança Corporativa foi aplicada nas ações com os Diretores, Conselho de administração e do Presidente, para evitar problemas maiores para a estrutura da empresa, principalmente quando foi percebido que o processo de aquisição de equipamento de TI estava parado, e a falta de ação na aquisição destes poderia afetar a estrutura de negócio, podendo comprometer o funcionamento de processos vitais para a empresa.

Com a renovação do parque tecnológico, após a chegada dos equipamentos novos relatados nesse estudo, o Departamento de Tecnologia da Informação teve condições de desenvolver um planejamento de instalações dos equipamentos, para evitar riscos futuros aos clientes da empresa, devido sua necessidade de acesso aos recursos de TI.

Este estudo mostrou o cuidado que os dirigentes dessa empresa tiveram com relação à identificação de conflito de interesses, baseados na teoria da agência, nas ações e preocupações para efetivar os investimentos em TI, com a finalidade de garantir a Gestão da Continuidade do negócio para a empresa.

Quanto à gestão de riscos que foi elaborada pela equipe de TI, essa se tornou a maneira pelo qual foi desdobrado o processo de aquisição. As influências da Governança Corporativa, como fator positivo das ações de gestão adotado pela empresa, garantiu a decisão apoiada no zelo pela sobrevivência da organização. Posteriormente, outros investimentos foram realizados em conjunto com essa filial como: a instalação de Geradores de energia e *nobreaks*, que pudessem garantir o funcionamento de todos os equipamentos do *Data Center*, devido a constantes quedas de energia ocorridas na região, para garantir a Gestão da Continuidade do Negócio.

REFERÊNCIAS

ANDRADE, Daniel et al. (2011). *Plano de contingência de TI: preparando sua empresa para reagir a desastres e manter a continuidade do negócio*. FacSENAC/DF, Pós-Graduação em Segurança da Informação da FacSENAC/DF. Distrito Federal-Brasil: Faculdade SENAC.

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

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

BRITO, Osias. (2010). *Gestão de riscos: Uma abordagem orientada a riscos operacionais*. 1ª Ed. São Paulo: Ed. Saraiva.

GUIMARÃES, I. C. (2006). *Uma pesquisa de campo sobre a contribuição da controladoria à gestão de riscos nas empresas não-financeiras de capital aberto da cidade de São Paulo*. Dissertação (Mestrado em Controladoria e Contabilidade Estratégica) - Centro Universitário Álvares Penteado, São Paulo.

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

IBGC - Instituto Brasileiro de Governança Corporativa. Recuperado em 01 de outubro, 2016, de <<http://www.ibgc.org.br/>>.

JENSEN, M. C. & MECKLING, W. H (1976). Theory of the firm: managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics*. v. 3, n. 4, p. 305-360.

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

RICHARDSON, Roberto Jarry (1999). *Pesquisa social: métodos e técnicas*. São Paulo: Ed. Atlas.

ROSSETI, José Paschoal & ANDRADE Adriana (2014). *Governança Corporativa: fundamentos, desenvolvimento e tendências*. São Paulo: Ed. Atlas.

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

SILVA, Marcelo Gaspar Rodrigues (2013). *TI: mudar e inovar: resolvendo conflitos com ITIL v3: aplicado a um estudo de caso*. Brasília: Senac DF.

SILVA, Marcelo Gaspar Rodrigues & GOMEZ, Thierry Albert M. Pedroso & MIRANDA, Zailton Cardoso de. (2013) TI: mudar e inovar: resolvendo conflitos com Itil, aplicando a um estudo de caso. Brasília: Senac DF.

SILVEIRA, Alexandre Di Miceli da. (2010). Governança Corporativa no Brasil e mundo: teoria e prática. Rio de Janeiro: Elsevier.

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