Gestão estratégica da qualidade da informação em processos operacionais na construção civil

Leonardo Fabris Lugoboni (FECAP; FEA-USP) leo_fabris@hotmail.com
Marcus Vinicius Moreira Zittei (FECAP; FURB) marcuszittei@zittei.com.br
Mônica Viana Callegari (FECAP) mviana.call@gmail.com
Marilia Neumann Couto (UTFPR) mariliancouto@gmail.com
Regina Aparecida Neumann (FECAP) regina.neumann@fecap.br

Resumo:
A finalidade desta pesquisa foi realizar um levantamento teórico sobre a gestão da informação, a segurança da informação, a qualidade da informação e o gerenciamento de riscos da informação. O objetivo foi verificar como as empresas do setor de construção civil estão gerenciando suas informações internas e como estão lidando com os riscos decorrentes de falhas na disponibilidade, na integridade e na confidencialidade das informações. Os dados dessa pesquisa foram analisados através de dezessete entrevistas realizadas com colaboradores de duas empresas de grande porte do setor de construção civil. Chegou-se à conclusão de que as empresas têm ciência da importância da qualidade da informação e do gerenciamento dos riscos decorrentes da informação, porem elas não possuem uma política de gerenciamento de riscos da informação adequada e não gerenciam as regras já estabelecidas referente à segurança da informação.
Palavras chave: Gestão da Informação, Segurança da Informação, Riscos da Informação, Qualidade da Informação, Construção Civil.

Strategic management of information quality in operational processes in building

Abstract
The purpose of this research was to perform a theoretical survey of the information management, information security, information quality and information risk management. The objective was to establish how C\civil construction companies manage their internal information and how they deal with the risks of failures on the availability, integrity and confidentiality of information. The data from this survey was analyzed through seventeen interviews with employees from two large companies in the construction sector. The conclusion was that the companies are aware of the importance of information quality and management of risks arising from information, however they do not have a relevant policy of information risk management and do not manage the rules already established regarding information security.
Key-words: Information management, Information security, Information risk, Information quality, civil construction.

1. Introdução

O sistema de informação estratégico é utilizado no gerenciamento da informação e no processo da tomada de decisão. Este sistema representa a evolução natural dos sistemas de informação em decorrência das necessidades empresariais em processar a informação recolhida, focando a vantagem competitiva e redefinição dos objetivos da empresa para reajustá-la às alterações ambientais.

Desta forma, os processos e mecanismos que traduzem a estratégia corporativa para a realidade, por meio de decisões e ações gerenciais têm sido analisados na política de planejamento. É possível definir as etapas da transição da estratégia de ação como: Estratégia, planejamento, orçamento e ação executiva. Os estágios de transição estão ligados por estrutura, processos e conteúdo. (CAMILLUS, 1981).

Contudo o ambiente competitivo organizacional gera um clima de incerteza para a tomada de decisões, estimulando os profissionais a procurarem entender de modo mais amplo as contribuições que as tecnologias podem oferecer à gestão estratégica da informação (MORAES, TERENCE e FILHO, 2004). Podemos entender Gestão Estratégica de Informação como um processo de busca e utilização de informações externas e internas para subsidiar decisões estratégicas. (BARBOSA, 1997).

Podemos dizer que a gestão da informação engloba a sinergia entre a tecnologia da informação, a comunicação e os recursos/conteúdos informativa, visando o desenvolvimento de estratégias e a estruturação de atividades organizacionais. Portanto, a gestão da informação implica em mapear as informações necessárias, fazer sua coleta, avaliar sua qualidade, proceder ao seu armazenamento e à sua distribuição e acompanhar os resultados de seu uso. (MORAES, TERENCE e FILHO, 2004).

Porem a vulnerabilidade ou a utilização indevida da informação pode oferecer grandes riscos às organizações. Pois a segurança da informação é imprescindível no ambiente estratégico organizacional e no ambiente competitivo de mercado.Para que as organizações obtenham sucesso no quesito segurança da informação, esta deve estar integrada com todos os níveis da organização e alinhada com os objetivos estratégicos estabelecidos no planejamento da administração organizacional (RICCIO, SAKATA e VALENTE, 2011).

De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), o risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. O resultado das iniciativas de negócios revela que o risco pode ser gerenciado a fim de subsidiar os administradores na tomada de decisão, visando alcançar objetivos e metas dentro do prazo, do custo e das condições pré-estabelecidas. (IBGC, 2007).

Conforme Teller e Kock (2013), as gestões empresariais que analisam os riscos oriundos da deficiência das informações são capazes de impor e influenciar as decisões. Consequentemente, o processo de tomada de decisão se torna mais profundo e mais rápido.

Muitas pessoas pensam que segurança da informação se resume à compra de equipamentos e sistemas caros, como firewalls, sistema de detecção de intrusos ou antivírus. Outras acham que incluir a adoção de políticas de segurança e o estabelecimento de responsabilidades funcionais ao aparato tecnológico é suficiente. Mas nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconsequente. Segurança da informação não é uma ciência exata. Se fossemos classifica-la, ela estaria no campo de gestão de riscos. E para gerir riscos é preciso conjugar vários verbos: conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar são apenas alguns deles. (SÊMOLA, 2014).

Portanto o objetivo geral deste trabalho é verificar como as empresas do segmento da Construção Civil gerenciam a qualidade e os riscos da informação.

De forma geral os fatores que levam riscos de informação nas companhias são comuns, mas de acordo com o ramo de atividade eles podem variar, e na construção civil um dos fatores mais relevantes da segurança da informação é a distância entre as obras e a administração que define o planejamento.

As obras e os departamentos administrativos podem ficar comprometidos quando os processos são ineficazes ou, quando as ferramentas administrativas são inadequadas, ou mesmo quando a comunicação das informações é feita de forma inadequada por colaboradores, influenciando na qualidade das informações disponibilizadas para os embasamentos na tomada de decisão.

Tendo em vista o cenário apresentado, esta pesquisa busca verificar qual é a melhor forma de gestão da qualidade da informação a se utilizar como planejamento estratégico, visando o crescimento e desenvolvimento das empresas, e como estas gerenciam os riscos ocasionados pela falta de gestão da informação no setor de construção civil.

2. Referencial Teórico

2.1 Gestão da Informação

Historicamente, a gestão da informação acontecia através de métodos de análise e projetos de sistemas que enfocavam dados e processos. Dessa ênfase inicial em algoritmos, programas e processos, as metodologias de desenvolvimento migraram para uma abordagem centrada nos dados. Posteriormente, as preocupações dos analistas e dos usuários foram passando dos dados operacionais para as informações agregadas envolvidas no processo de tomada de decisão. Assim, a gestão da informação evoluiu para se tornar um apoio na tomada de decisão em situações de negociação (MACAGNAN e LINDEMANN, 2009).

Por isso, o conceito de tecnologia da informação deve ser compreendido como sendo muito mais amplo do que apenas considerá-la como processamento de dados, engenharia de software, informática ou o conjunto de hardware e software, devendo ser considerados aspectos humanos, administrativos e da organização (BORGES, PARISI e GIL, 2005).

Desta forma, a gestão da informação requer o estabelecimento de processos, etapas ou fluxos sistematizados e estruturados, associado às pessoas responsáveis por sua condução, para que se obtenham os resultados almejados. Os fluxos de informação permitem o estabelecimento das etapas de obtenção, tratamento, armazenamento, distribuição, disseminação e uso da informação no contexto organizacional (VITAL, FLORIANI e VARVAKIS, 2010).

Segundo o Tribunal de Contas da União, a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações (TCU, 2012).

Estes pontos deficitários podem ser melhorados através de uma melhor gestão da informação, com base em dados que muitas vezes já estão dentro da empresa e não são explorados de forma adequada para proporcionar crescimento, evitando a estagnação ou, até mesmo, a um prematuro encerramento de suas atividades (KRAFTA e FREITAS, 2008).

Agora sabemos o quão valioso é a informação para o negócio, mas temos de dissecar todos os

aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle e, principalmente, os momentos que fazem parte de seu ciclo de vida. Toda informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade e legalidade, que complementam essa influência. O ciclo de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação sustentando processos que, por sua vez, mantêm a operação da empresa (SÊMOLA, 2014).

Assim, a Gestão de Informação pode ser definida como um conjunto estruturado de atividades que incluem o modo como as empresas definem, obtêm, distribuem e usam a informação (COSTA e MAÇADA, 2009).

2.2 Segurança da Informação

A segurança e o controle dos sistemas de informações requerem o comprometimento de todos os envolvidos no processamento de dados, desde o provedor da informação ao receptor da mesma (BORGES, PARISI e GIL, 2005).

Conforme o Tribunal de Contas da União (TCU, 2012), a segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. E define cada uma como:

Integridade - Fidedignidade das informações. Conformidade dos dados. Garantia de não violação.

Confidencialidade - Garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação.

Autenticidade - Garantia da veracidade da fonte das informações.

Disponibilidade - Garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática.

A Tecnologia da Informação deve efetivamente contribuir para minimizar as perdas e potencializar os investimentos. Por outro lado, a Gestão de Riscos e seu planejamento deixaram de ser apenas técnica e requer dos demais gestores o compromisso para com a informação. É no trabalho de equipe, com uma cultura de controle de riscos em todos os níveis da organização, que serão encontradas as melhores alternativas para se manter a segurança da informação de forma compatível com seu valor dentro da organização (FREITAS, 2009).

Assim podemos definir segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, podemos também considera-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Dessa forma, estaríamos falando da definição de regras que incidiram sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades (SÊMOLA, 2014).

2.3 Gestão de Risco na Qualidade e Segurança da Informação

Após verificarmos a importância da gestão e da segurança da informação, agora podemos

abordar os riscos por falhas na segurança da informação.

Para Sêmola (2014), podemos classificar as ameaças à informação quanto a sua intencionalidade, e podem ser divididas nos seguintes grupos:

Naturais: Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.

Involuntárias: Ameaças inconsistentes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.

Voluntárias: Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Assim identificar os riscos importa em identificar as ameaças e as vulnerabilidades que podem ser aproveitadas por estas aos sistemas de informação envolvidos e o impacto que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos (FREITAS, 2009).

Portanto no gerenciamento das operações, mostra-se fundamental existir a documentação dos processos, como forma de harmonizar e padronizar a realização das atividades. Da mesma forma, o registro (transparente a todos os atores do processo) do status de cada atividade auxilia os envolvidos a gerenciarem atividades predecessoras e sucessoras a uma atividade em andamento, além de conferir confiabilidade ao processo das informações (LUCIANO e TESTA, 2011).

Em termos estratégicos, a segurança da informação pode agregar valor ao dar maior confiabilidade ao próprio processo de transformação. A integração entre o negócio e a tecnologia empregada pode imprimir maior maturidade e solidez às transações com o cliente. A confiabilidade nas transações vai se traduzir na ideia de maior confiabilidade nos negócios (FREITAS, 2009).

Pode-se dizer que se os sistemas de gestão da informação não são eficientes, é grande a probabilidade de existir assimetria das informações, cujas consequências podem levar a problemas de risco moral. Estes problemas acabam por intervir negativamente nos resultados econômicos (MACAGNAN e LINDEMANN, 2009).

Outro risco que podemos abordar é o risco de perda de informações. De acordo com Krafta e Freitas (2008) o fato de duas ou mais bases de informações estarem ativas simultaneamente pode gerar trabalho em excesso, pois as pessoas que manipulam as bases precisam consultar e preencher mais de um local, aumentando o risco de perda de informação.

Para um bom tratamento da informação, podemos ver que um dos segredos é a análise dos riscos antecipada. Conforme Martins e Santos (2005) o Gerenciamento de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes. Assim a análise de riscos pode ser tanto quantitativa - baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança - quanto qualitativa - baseada em know-how e geralmente realizada por especialistas. Não é possível afirmar com certeza qual é a melhor abordagem, uma vez que cada uma delas fornece uma ferramenta valiosa para a estruturação das atividades de identificação de riscos.

Para Lunardi, Becker e Maçada(2010) o uso de práticas de *compliance* também foi apontado como um mecanismo de forte impacto sobre a gestão da TI. Pressionadas por diferentes órgãos reguladores, muitas organizações têm se preocupado em garantir a conformidade dos seus processos internos, visto que podem ser auditadas e cobradas por esses órgãos a qualquer

momento. Mesmo que não seja responsabilidade exclusiva da área de TI, muitos dos pontos a serem auditados estão relacionados ou são dependentes da TI, como o acesso e a segurança às informações, e a integridade dos sistemas (como o uso de planilhas eletrônicas que ficam sendo manipuladas fora dos sistemas da organização).Com o cumprimento dessas exigências, vários benefícios acabaram atingindo a área de TI, como: a redução do risco de fraudes, a revisão de procedimentos, o desenvolvimento de práticas mais eficientes e uma melhor distribuição de responsabilidades – aspectos anteriormente considerados pela alta administração como superficiais.

Assim verificamos que todos os riscos relacionados à Gestão da Informação estão interligados, pois os ataques contra a confidencialidade podem ter por resultado a liberação de informação não autorizada para fins de divulgação ou fraude. Ataques contra a integridade irão contra a confiabilidade da informação. E ataques contra a disponibilidade irão contra o suporte ao serviço ou a destruição da informação (FREITAS, 2009). Por este motivo o Plano de Segurança da Informação deve ser bem definido, pois a falha em um processo pode resultar em diversos riscos para a empresa.

É fundamental que todos tenham a consciência de que não existe segurança total e, por isso, devemos estar bem estruturados para suportar mudanças nas variáveis, reagindo com velocidade e ajustando o risco novamente aos padrões especificados como ideais para o negócio (SÊMOLA, 2014).

Os riscos apontados até o momento são generalizados a qualquer tipo de empresa. Porem a Construção Civil tem riscos específicos do setor. E conforme Nascimento e Santos (2002), dado o tamanho do setor, suas características de uso intensivo de informação e a atual ineficiência de comunicação e baixa produtividade, os benefícios na integração da TI aos processos do setor seriam enormes. Infelizmente, há barreiras de diversas naturezas que ainda impedem a adoção generalizada destas tecnologias pela indústria da construção, como por exemplo, os profissionais recrutados têm perfis diferentes aos das outras indústrias e com menos exigências, a verificação das informações é feita e corrigida muitas vezes pela mão de obra operacional. Porém o potencial de utilização da TI na indústria da Construção é muito grande.

2.4 A Qualidade da Informação como Gestão Estratégica

Após a globalização e o surgimento da informática, o cenário econômico mundial tornou-se mais competitivo. Passou-se de uma economia industrial para uma economia de informação, de modo que as empresas que não se informatizam perdem lugar no mercado muito rapidamente. As empresas precisam saber como gerenciar a informação interna, para conseguir alcançar diferencial competitivo no mercado (ANDREASI e GAMBARATO, 2010).

Contudo o atual cenário empresarial demonstra que a informação, seja qual for o mercado ou área de atuação da organização, vem assumindo crescente importância estratégica, tanto pela globalização dos mercados quanto pela rapidez com que as informações circulam e as mudanças ocorrem (KRAFTA e FREITAS, 2008).

Pois a rapidez, produtividade e inovação são características difíceis de serem construídas por suas naturezas conflitantes. Rapidez e produtividade são congruentes, mas adicionar a capacidade de inovação simultaneamente parece dicotômico (RODRIGUES, MACCARI e SIMÕES, 2009).

Desta forma, a Gestão da Informação pode auxiliar a agilidade e a eficiência, e conforme Slack, Chambers e Johnston(2002) pode ser utilizada como um Sistema de Apoio à Decisão, que é aquele que fornece informação com o objetivo direto de adicionar ou apoiar o processo

decisório gerencial. Consegue isso estocando informação importante, processando-a, e apresentando-a de forma que possa contribuir para a decisão a ser tomada.

Pois os riscos para o negócio ocasionados pela vulnerabilidade da informação estratégica inerentes a um ambiente de TI passam muitas vezes despercebidos e isso pode reduzir consideravelmente a competitividade da empresa. Tal situação remete à necessidade de uma abordagem da segurança da informação não somente no nível operacional como normalmente é realizada, mas também em nível estratégico em qualquer organização (RICCIO, SAKATA e VALENTE, 2011).

Assim, reunir gestores com visões do mesmo objetivo, mas de pontos distintos, é fundamental para a obtenção da nítida imagem dos problemas, desafios e impactos. Por isso, envolver representantes das áreas tecnológicas, de comunicação, comercial, de negócios, jurídica, patrimonial, financeira, de auditoria etc. em muito agregará para o processo de gestão, de forma a evitar conflitos, desperdícios, redundâncias, e o principal: fomentar a sinergia da empresa, o que intimamente alinha as suas diretrizes estratégicas de curto, médio e longo prazos (SÊMOLA, 2014).

3. Metodologia

A metodologia empregada caracteriza-se como pesquisa qualitativa exploratória, pois é um estudo de natureza analítica e não estatística. Trata-se de um estudo de caso, que é uma abordagem de pesquisa que procura atender as questões do tipo "como" e "por que" tal fenômeno ocorre em determinado contexto (Yin, 1994), utilizando entrevistas semiestruturadas feitas com colaboradores de duas empresas de grande porte do Setor da Construção Civil.

As entrevistas foram realizadas com colaboradores de todos os setores, como Financeiro, Planejamento, Contabilidade, Departamento Pessoal, Suprimentos, Depósito e Obras. E com todos os níveis de cargos como Assistentes, Analistas, Encarregados e Gestores, conforme o quadro (1).

	Empresa A				**Empresa B**			
	Assistentes	Analistas	Encarregados	Gestores	Assistentes	Analistas	Encarregados	Gestores
Financeiro	1	1	-	-	-	1	1	-
Planejamento	-	1	-	1	-	1	-	-
Contabilidade	-	1	1	-	1	1	-	1
Depto Pessoal	-	1	-	-	-	1	-	-
Suprimentos	-	-	-	-	1	-	-	-
Depósito	-	-	-	-	1	-	-	-
Obras	-	-	1	-	-	-	-	-

Quadro (1) – Relação de Cargos e Departamentos das entrevistas efetuadas.

Assim esta pesquisa busca verificar qual é a melhor forma de gestão da qualidade da informação a se utilizar como planejamento estratégico, bem como as empresas gerenciam os riscos ocasionados pelas ameaças à gestão da informação no setor de construção civil.

4. Análise dos Dados

As empresas em estudo têm as sedes localizadas na cidade de São Paulo, porém possuem obras em andamento em várias cidades do Brasil como: São Paulo, São José dos Campos, Campinas, Cubatão, Manaus, Araucária, Betim, entre outras.

A “empresa A” possui mais de 40 anos de mercado, com aproximadamente setecentos colaboradores internos e mil colaboradores terceirizados. Considerada uma empresa de grande

porte do setor de Construção Civil, possui maior operação na área de Edificações e Estruturas. Encontra-se em fase de reestruturação dos objetivos com foco no crescimento em outros setores da área de Construção Civil.

A "empresa B" possui quase 30 anos de mercado, com aproximadamente dois mil colaboradores internos. Considerada uma empresa de grande porte do setor de Construção Civil, possui maior operação na área Industrial e de Manutenções.

Verificou-se na literatura pesquisada, o quão importante é a Gestão da Informação nas empresas. E como sua utilização e disponibilidade podem acarretar em riscos para a organização. De acordo com os colaboradores entrevistados, observou-se que todos têm conhecimento desta importância e que a administração das empresas tem preocupação com o assunto.

Conforme os colaboradores da "empresa A", existe um portal Intranet onde todas as informações são armazenadas e podem ser consultadas apenas por pessoas autorizadas de acordo com a necessidade de cada área, e a política de segurança da informação é devidamente divulgada. Já na "empresa B", os colaboradores têm ciência da importância da segurança da informação, porém não souberam explicar como funciona a política da empresa.

Com relação à responsabilidade da Segurança da Informação, há uma dificuldade na definição, pois tanto na "empresa A", como na "empresa B" cada colaborador respondeu à esta pergunta de forma diferente. Alguns acreditam que seja de responsabilidade do departamento de TI, porém outros acreditam que seja de responsabilidade de todas as áreas, onde cada área tem a sua participação. Conforme Sêmola (2014), a segurança da informação é de responsabilidade de todas as áreas, onde as junções de todas as opiniões geram melhores resultados e diminuem os riscos. Desta forma podemos ver uma falha na comunicação da política de segurança de informação, pois obtemos respostas diversas, não obtendo sinergia entre as áreas.

Referente ao fluxo de informações entre as diversas áreas verificou-se que tanto a "empresa A", como a "empresa B", os colaboradores não têm conhecimento de como as demais áreas funcionam, armazenam ou geram as informações. Cada colaborador tem acesso apenas às informações geradas por sua área. Apenas os Gestores têm acesso a todas as informações e repassam conforme a necessidade. Devido à isto, apenas eles possuem conhecimento de todo o fluxo de informações.

Neste caso, temos de um lado a segurança de que a informação não passará por pessoas não autorizadas, porém a restrição na disponibilidade da informação poderá implicar em dificuldades e atrasos nos processos da empresa. Conforme Vital, Floriani e Varvakis (2010) deve-se estabelecer processos dos fluxos de informações e divulga-los para sinergia das áreas.

Já considerando a linguagem do fluxo de informações, podemos ver que este método de apenas os gestores terem acesso às informações de outras áreas, facilita na hora de repassar aos colaboradores. Pois desta forma o gestor de cada área repassa apenas o essencial para o trabalho de cada um, este "filtro" facilita a compreensão das informações por todos.

Observou-se também, que ambas as empresas incentivam os funcionários a repassar os conhecimentos. Com o intuito de ter uma pessoa "backup" para casos de ausência de um colaborador. Podemos considerar este procedimento como uma prevenção para garantir a agilidade e eficiência nos processos da empresa, conforme o Gestor Contábil da "empresa B".

Com relação aos comunicados gerais, a "empresa A" utiliza um portal Intranet restrito a funcionários e a formalização das informações por e-mail, assim nos informou a Analista Financeiro. Já a "empresa B" também utiliza o e-mail e os murais informativos que são

espalhados pela empresa e obras, conforme o Assistente de Suprimentos.

Agora vamos abordar os sistemas de informação utilizados pelas empresas. Ambas utilizam um sistema ERP, onde cada área tem um modulo que deve ser alimentado com as informações respectivas das áreas, e o sistema tem o objetivo de integrar essas informações para atender os Órgãos Públicos e ajudar na Gestão da Empresa. Nas duas empresas os acessos aos módulos são restritos para cada colaborador conforme a função e a área de atuação. Apenas os gestores têm acessos às informações de outros departamentos, porém eles possuem somente acesso de visualização, pois as inclusões e alterações das informações são restritas a cada área.

Na "empresa A" todos os colaboradores dizem que o sistema é de fácil utilização, que todas as informações necessárias são obtidas com agilidade e consistência. Todos os funcionários responderam que receberam os treinamentos e cursos devidos para manuseio do sistema. A única dificuldade encontrada foi nos relatórios gerados pelo sistema, forçando-os a utilizar planilhas e controles externos em alguns casos. Mas de maneira geral, a "empresa A" utiliza poucos controles externos ao sistema de informação utilizado na organização, assim a maior parte das informações são centralizadas no sistema.

Já na "empresa B" todos os colaboradores informaram ter muitas dificuldades com relação à utilização do sistema de informação. Eles têm dificuldades de obter informações, pois não tiveram o treinamento devido. Conforme a Analista Fiscal, "a necessidade de controles externos é grande, pois não se pode confiar nos relatórios gerados pelo sistema".

Conforme literatura pesquisada, a "empresa B" corre grandes riscos de integridade e autenticidade das informações. Conforme o TCU (2012) estes riscos podem comprometer significativamente o andamento dos próprios processos institucionais. Outra ameaça relacionada a este caso do mau uso do sistema de informação e a necessidade de controles externos, é o risco de perda de informações, que de acordo com Krafta e Freitas (2008) o fato de duas ou mais bases de informações estarem ativas simultaneamente pode gerar trabalho em excesso, pois as pessoas que manipulam as bases precisam consultar e preencher mais de um local, aumentando o risco de perda de informação.

Ao abordarmos o tema Gerenciamento de Riscos, questionamos se as empresas tinham algum tipo de projeto relacionado a isto. Todos os departamentos responderam apenas sobre a política de riscos de acidentes nas obras. Que nas duas empresas é tratado com grande importância, acima de qualquer outro tipo de risco. O único departamento preocupado com riscos de informação, foi o departamento de planejamento financeiro. Que abordou apenas os riscos financeiros decorrentes de falhas nas informações. Porém, nenhuma das empresas tem uma política de gerenciamento de riscos da informação.

Conforme Sêmola (2014) é fundamental que todos tenham a consciência de que não existe segurança total e, por isso, devemos estar bem estruturados para suportar mudanças nas variáveis, reagindo com velocidade e ajustando o risco novamente aos padrões especificados como ideais para o negócio.

E para isto ocorrer, é imprescindível que a empresa tenha uma política de gestão de riscos de informação, e que ela seja disseminada por toda a empresa.

Desta forma, também devemos verificar se a distância entre as obras e a sede, pode ser um risco para a empresa.

Mais uma vez, para a "empresa A" isto não é considerado um problema. Pois, conforme o Analista de Planejamento, "as informações disponibilizadas no sistema e a comunicação entre as áreas não é considerada uma dificuldade".

Já para a "empresa B", o problema sistêmico e a falta de treinamento dos colaboradores podem se tornar um risco para a empresa com relação a distância entre as obras. Todos os colaboradores apontaram dificuldades com relação a distância. Como, por exemplo, a Analista do Departamento Financeiro apontou que "muitas vezes a operação fica parada por conta dos colaboradores das obras não transmitirem as informações em tem hábil". Pois a maioria das informações são repassadas via e-mail, já que o sistema não é "alimentado" corretamente.

Quando entramos na questão de confidencialidade das informações, ambas as empresas apontam este tema como de extrema importância. Porém como já analisamos outros pontos de riscos, e podemos ver que principalmente a "empresa B" corre grandes riscos com relação à confidencialidade de suas informações. Pois a sua deficiência com relação a ter muitos controles externos ao sistema e a falta de orientação, ou devido treinamento, de seus colaboradores, pode sim colocar em risco a confidencialidade de suas informações.

Conforme Sêmola (2014) toda informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade e legalidade, que complementam essa influência, que por sua vez, mantêm a operação da empresa.

Todos os colaboradores foram unanimes em afirmar que a qualidade da informação pode sim influenciar em uma tomada de decisão, conforme observou-se na literatura pesquisada, a informação com qualidade pode ser utilizada como um Sistema de Apoio à Decisão, que é aquele que fornece informação com o objetivo direto de adicionar ou apoiar o processo decisório gerencial (SLACK, CHAMBERS e JOHNSTON, 2002).

"As decisões devem ser tomadas com base em informações claras e de qualidade, pois assim elas terão um suporte melhor para atingir seu objetivo" - Analista de planejamento da "empresa A".

"As informações sem consistência podem levar a uma tomada de decisão errada, e isto poderá trazer graves problemas para a empresa" - Analista financeiro da "empresa B".

A analista fiscal da "empresa B" já destacou a continuidade da empresa, abordando que falhas na informação podem prejudicar a formação de custo dos projetos, colocando em risco os resultados financeiros da empresa, assim influenciando fortemente na tomada de decisão dos gestores.

Assim como a encarregada do financeiro da "empresa A" considerou que a qualidade nas informações pode habilitar a empresa a alcançar seus objetivos pelo uso eficiente dos recursos disponíveis, assim a informação é essencial para o sucesso num ambiente de concorrência.

Cada um abordou um tema de relevância na empresa, o que nos mostra como a qualidade da informação pode beneficiar e influenciar todos os setores da empresa. E como a sua falta poderá causar vários riscos a continuidade do negócio.

Assim confirma-se a teoria de Riccio, Sakata e Valente (2011), onde afirmam que os riscos para o negócio ocasionados pela vulnerabilidade da informação estratégica inerentes a um ambiente de TI passam muitas vezes despercebidos e isso pode reduzir consideravelmente a competitividade da empresa.

5. Considerações finais

Esta pesquisa teve como objetivo verificar qual é a melhor forma de gestão da qualidade da informação a se utilizar como planejamento estratégico, bem como as empresas gerenciam os riscos ocasionados pela falta de gestão da informação no setor de construção civil.

As empresas tem conhecimento da importância da informação, dos riscos que a falta de gestão da informação podem acarretar a empresa, porém, nem a "empresa A" e nem a "empresa B" gerenciam a informação com a devida importância.

A "empresa A" se preocupa um pouco mais com os processos de gerenciamento de informação, treinando seus usuários e se preocupando em restringir o acesso a qualquer colaborador, porém, também não possui uma política de gerenciamento de riscos, criando uma vulnerabilidade.

A "empresa B" já está correndo vários riscos com relação falta de gerenciamento de informação. Notou-se que existe uma preocupação da empresa com relação a isto, porém não há nenhuma atividade de prevenção ou gerenciamento de riscos.

Nenhuma das empresas tem um planejamento definido para auxiliar no gerenciamento de riscos de informações. Existe uma política de segurança das informações, onde são abordadas algumas regras para minimizar riscos, porém não há controle de como essas regras são executadas.

Para Sêmola (2014), a Gestão da Informação é de extrema importância, e seu gerenciamento deve ser prioritário entre todas as áreas da empresa, para obter a sinergia de opiniões, visando melhorias nos processos. Deve-se fazer o levantamento de riscos constantemente, e gerenciar os riscos da melhor forma possível. Pois não há como não ter riscos, eles apenas podem ser minimizados.

Referências

ANDREASI, M.S.; GAMBARATO, V.T.S. Uso Da Tecnologia Da Informação Como Vantagem Competitiva Nas Organizações. **Tékhne ε Lógos**, Botucatu, SP, v.1, n.2, fev. 2010.

BARBOSA, R. R. Monitoração Ambiental: uma Visão Interdisciplinar. **Revista de Administração**, São Paulo: v.32, n.4, p. 42-53, 1997.

BORGES, T.N.; PARISI, C.; GIL, A.D.L. O Controller como Gestor da Tecnologia da Informação - Realidade ou Ficção? **Revista de Administração Contemporânea**, Rio de Janeiro, v. 9, n. 4, p. 119-140,Oct 2005.

CAMILLUS, J.C. Corporate strategy and executive action: Transition stages and linkage dimensions. **Academy of Management. The Academy of Management Review (pre-1986)**, Briarcliff Manor, v. 6, n. 2, p. 253, 04 1981.

COSTA, J.C.; MAÇADA, A.C.G. Gestão Da Informação Interorganizacional Na Cadeia De Suprimentos Automotiva/Interorganizational Information Management In The Automotive Supply Chain. **RAE - Eletrônica**, São Paulo, v. 8, n. 2, p. 1-25, Jul 2009.

FREITAS, E.A.M. Gestão De Riscos Aplicada A Sistemas De Informação: Segurança Estratégica Da Informação. **Biblioteca Digital da Câmara dos Deputados**, 2009.

IBGC - Instituto Brasileiro De Governança Corporativa. **Guia de orientação para gerenciamento de riscos corporativos**. São Paulo: p. 11, 2007.

KRAFTA, L.; FREITAS, H. Ação Comercial Baseada Na Gestão Da Informação De Uma Pequena Empresa De TI/Commercial Action Based On Information Management In A Small It Company. **Journal of Information Systems and Technology Management: JISTEM**, Sao Paulo, v. 5, n. 3, p. 483-503, 2008.

LUCIANO, E.M.; TESTA, M.G. Controles De Governança De Tecnologia Da Informação Para A Terceirização De Processos De Negócio: Uma Proposta A Partir Do Cobit/ControlsOfInformation Technology Management For Business Processes Outsourcing BasedOnCobit. **Journal of Information Systems and Technology Management : JISTEM**, Sao Paulo, v. 8, n. 1, p. 237-262, 2011.

LUNARDI, G.L.; BECKER, J.L.; GASTAUD MAÇADA, A.C. Impacto da adoção de mecanismos de governança de Tecnologia de Informação (TI) no desempenho da gestão da TI: uma análise baseada na percepção dos executivos. **Revista de Ciencias da Administracao**, Florianopolis, v. 12, n. 28, p. 11, Sep 2010.

MACAGNAN, C.B.; LINDEMANN, A. Gestão Da Informação E O Processo De NegociaçãoBancária/Administration Of The Information And The Process Of Bank Negotiation. **Journal of Information Systems and Technology Management : JISTEM**, Sao Paulo, v. 6, n. 1, p. 93-109, 2009.

MARTINS, A.B.; SANTOS, C.A.S. Uma Metodologia Para Implantação De Um Sistema De Gestão De Segurança Da Informação/A MethodologyToImplementAnInformation Security Management System. **Journal of Information Systems and Technology Management : JISTEM**, Sao Paulo, v. 2, n. 2, p. 121-136, 2005.

MORAES, G.D.D.A.; TERENCE, A.C.F.; FILHO, E.E. A Tecnologia Da Informação Como Suporte À Gestão Estratégica Da Informação Na Pequena Empresa/Information Technology As A SupportTo The Strategic Management OfInformation In Small Businesses. **Journal of Information Systems and Technology Management: JISTEM**, São Paulo, v. 1, n. 1, p. 28-44, 2004.

NASCIMENTO, L. A.; SANTOS, E. T. Barreiras para o uso da tecnologia da informação na indústria da construção civil. In: WORKSHOP NACIONAL DE GESTÃO DE PROCESSO NA CONSTRUÇÃO DE EDIFÍCIOS, Porto Alegre. PUC, 2002.

RICCIO, E.L.; SAKATA, M.C.G.; VALENTE, N.T.Z. Resultados do 8º Contecsi - Congresso Internacional De Gestão Da Tecnologia E Sistemas De Informação/OutcomesOf The 8ThContecsi - InternationalConferenceOnInformation Systems And Technology Management. **Journal of Information Systems and Technology Management : JISTEM**, Sao Paulo, v. 8, n. 2, p. 471-507, 2011.

RODRIGUES, L.C.; MACCARI, E.A.; SIMÕES, S.A. O Desenho Da Gestão Da Tecnologia Da Informação Nas 100 Maiores Empresas Na Visão Dos Executivos De TI/It Management Design At The Top 100 Brazilian Companies, According To Their CIOs. **Journal of Information Systems and Technology Management : JISTEM**, Sao Paulo, v. 6, n. 3, p. 483-505, 2009.

SÊMOLA, M. Gestão da Segurança da Informação: uma visão executiva. **Editora Campus**, **2º edição.** Rio de Janeiro. Elsevier, 2014.

SLACK, N.; CHAMBERS, S.;JOHNSTON, R. Administração da produção. 2º ed., 747p.São Paulo: Atlas, 2002.

TCU - Tribunal De Contas Da União. Boas Práticas em Segurança da Informação, 4º edição**. Secretaria de Fiscalização de Tecnologia da Informação**, Brasília, 2012.

TELLER, J.; KOCK, A. An empirical investigation on how portfolio risk management influences project portfolio success. **International Journal of Project Management**, Kidlington, v. 31, n. 6, p. 817, 08 2013.

VITAL, L.P.; FLORIANI, V.M.; VARVAKIS, G. Gerenciamento Do Fluxo De Informação Como Suporte Ao Processo De Tomada De Decisão. **Inf. Inf.**, Londrina, v. 15, n. 1, p. 85 - 103, jul./jun. 2010.

YIN, R. K. Case study research: design and methods. 2nd ed. Newbury Park: Sage, 1994.