ANÁLISE DE GESTÃO DE RISCOS E IMPACTOS DA TECNOLOGIA DA INFORMAÇÃO NOS NEGÓCIOS

José Picovsky
Mestre em Direção Estratégica em Tecnologias da Informação, pela Fundação Universitária IberoAmericana, Lion, Espanha. Especialização em Administração Hospitalar pela Faculdade São Camilo, São Paulo,Brasil.Engenheiro Civil pela Faap São Paulo,Brasil.Especialização em Analise de Sistemas pela Faap São Paulo,Brasil. Professor de cursos universitários há mais de 20 anos. Atuando há mais de 10 anos em Hospitais e empresas da saúde.
jpicovsky@gmail.com

RESUMO
Hoje é facilmente perceptível entender porque os quadros executivos das corporações mundiais buscam incansavelmente respostas para a pergunta: Como mitigar os riscos e evitar transtornos decorrentes de problemas relacionados a Tecnologia da Informação nas organizações de Saúde?
Este tema é muito atual e é extremamente importante para avaliar o quanto o gerenciamento de riscos deve ser integrado às funções e aos grupos de funções da gestão da tecnologia da informação.
O gerenciamento de riscos deve ser executado continuamente no decorrer de todo o ciclo em todas as tarefas do dia-a-dia de maneira que as organizações possa conduzir seus negócios de uma forma segura no que se refere a utilização de computadores utilizados para apoio na gestão de negócios.

PALAVRAS-CHAVE: Exposição ao Risco, Riscos de Equipamentos**,** Tecnologia da Informação.

ANALYSIS OF RISK MANAGEMENT AND IMPACT OF INFORMATION TECHNOLOGY IN BUSINESS

RESUMO
Today is readily apparent to understand why executives of global corporations relentlessly seek answers to the question: How to mitigate risks and avoid inconvenience due to problems related to Information Technology in Health organizations?
This theme is very current and it is extremely important to assess how risk management should be integrated with functions and groups of functions of management of information technology.
Risk management should be run continuously during the whole cycle with all tasks of the day to day so that organizations can conduct their business in a secure manner as regards the use of computers used to support the management business.

Keywords: Risk Exposure, Equipments Risks, Information Technology

ANÁLISE DE GESTÃO DE RISCOS E IMPACTOS DA TECNOLOGIA DA INFORMAÇÃO NOS NEGÓCIOS

INTRODUÇÃO

A informática tem revolucionado a maneira de pensar de diversos empresários, pois os computadores vinham sendo utilizados como imensos armazenadores de dados mas hoje, a visão é explorar a informação como um meio para tomada decisões que norteiam a vida das empresas, além disto, outras modalidades de negócios estão surgindo com o advento da internet e extranets.

Compreender as formas pelas quais se podem aperfeiçoar o uso dos recursos informacionais e de Tecnologia da Informação (TI), representa hoje, um aspecto fundamental para a melhoria do desempenho de qualquer organização.

O departamento de TI deve entender profundamente do negócio e deve manter uma sinergia muito grande com todos os colaboradores organizacionais, com o objetivo de melhorar suas redes de informações internas, bem como, melhorar a qualidade dos serviços prestados tanto para os usuários internos como para os externos. [1]

Em paralelo às novas contribuições da informática, inúmeras manchetes têm sido publicadas com diversos problemas relacionados aos riscos tecnológicos, tais como : roubos de mídias de backup, processos litigiosos resultantes da produção e/ou preservação imprópria de registros eletrônicos,roubo de identidade, roubo de informações, quebras de propriedades intelectuais.

Alem disto, outros problemas, relacionados à tecnologia da informação (TI), tem incomodado diversos donos de empresas, diretores e gestores de diversas áreas que dependem da TI para dar continuidade nos seus negócios.

As infra-estruturas de TI quando mal dimensionadas ocasionam prejuízos enormes às instituições com paralisações de serviços, pois muitas vezes ocorrem problemas como: não existem servidores com capacidade de processar a informação necessária, estruturas que não garantem a segurança da informação, despreparo de profissionais da tecnologia da informação para lidar com a complexidade de problemas, compras de softwares que demandam alto custo para implantação ou customizações, empresas de prestação de serviços com TI que não cumprem aquilo que foi acordado, enfim estamos vivenciando uma era onde o amadorismo e as ações mal intencionadas podem comprometer todos aqueles que utilizam da informação eletrônica.

Os serviços de internet oferecidos pelos bancos agilizam pagamentos, transferência de recursos financeiros, propiciam aplicações com facilidades, diminuem as filas nas agencias. Ações de hackers conseguem deixar o sistema fragilizado com roubos ou ações

[1] Magalhães, Ivan Luizio; Pinheiro, Walfrido Brito,2007

que deixam os servidores tão sobrecarregados que não permitem que os serviços funcionem por tempo indeterminado.

As ações mal intencionadas conseguem alterar notas e faltas registradas nos computadores de escolas. Um email onde alguém o utilize indevidamente para ofender uma autoridade ou alguém da alta gestão de uma empresa pode comprometer pessoas e até mesmo a própria empresa.
Muitas empresas de software, por não estarem preparadas, implantam sistemas sem criar processos ou definir um rigor maior para fazer entregas de sistemas com um índice menor de problemas. Muitos destes problemas são oriundos da falta de um plano de testes de sistemas quanto aos atendimentos de requisitos de clientes, falha nos testes com volumes de dados que possam definir melhor a arquitetura do sistema, falha nos processos de documentações, falhas nos processo de segurança da informação, erros de gestão do projeto, enfim através destas falhas, muitas empresas de softwares acabam fechando as suas portas e deixam clientes cada vez mais preocupados quando há a necessidade da implantação de um novo software.

Hoje, é possível que alguém tire a vida de outra pessoa a distancia, como por exemplo, uma ação onde há uma substituição indevida de medicamentos num hospital, ou a troca de textos de laudos de exames.

Com o avanço da tecnologia, a informática deixou de ser algo apenas que agrega computadores locais nas redes de computadores mas podemos ter computadores remotos e outros equipamentos que são coordenados por algum computador da rede de micros. Isto ocorre em diversos segmentos, como por exemplo no ramo hospitalar onde bombas de infusão podem ser adicionadas a uma rede de computadores. A bomba de infusão é um aparelho médico-hospitalar ou veterinário usada para infundir líquidos, tais como drogas ou nutrientes em pacientes, com controle de fluxo e volume nas vias venosa, arterial ou esofágica.

Novamente, é possível uma ação má intencionada que possa comprometer a vida de um paciente.

Métodos

A pesquisa tem um caráter pragmático, é um "processo formal e sistemático de desenvolvimento do método científico. O objetivo fundamental da pesquisa é descobrir respostas para problemas mediante o emprego de procedimentos científicos". [2]

Vendo por um prisma mais filosófico, a pesquisa é uma atividade básica das ciências na sua indagação e descoberta da realidade. [3]

Desta forma, para este trabalho houve a opção de uma pesquisa bibliográfica elaborada a partir de material já publicado, constituído principalmente de livros, visando investigar a

[2] Gil, Antonio Carlos ,1991
[3] Minayo O, Maria Cecília de Souza

importância da gestão de riscos nos serviços da Tecnologia da Informação nas organizações.

Analise Crítica do Problema

Desde os primórdios do uso do computador para auxiliar os usuários nas suas atividades finais, a TI sempre se preocupou muito mais com o produto final para atender a uma demanda do que a concepção do mesmo. Poucos prestadores de serviços se preocupam, até hoje, com os riscos dos processos para conceber a uma necessidade do cliente e tão menos com a existência de riscos que possam comprometer um negócio quando da fase de implantação e continuidade da existência do produto agora fazendo parte do negócio de um cliente.

Para entender os que são riscos, precisamos distingui-lo, primeiro, do que é perigo. Podemos entender o perigo como uma fonte potencial de dano, como, por exemplo, um choque elétrico produzido por um equipamento durante procedimento cirúrgico. O risco é a estimativa da ocorrência de um dano onde são levadas em consideração a probabilidade de ocorrência do dano e a gravidade do mesmo.

Vários fatores podem desencadear um risco, entre eles uma determinada condição específica em se encontra um objeto do risco, uma falha decorrente por falta de manutenção do objeto do risco, enfim o prejuízo é o dano gerado a uma propriedade ou ao meio ambiente.

O gerenciamento de risco se compõe de atividades de identificação dos perigos existentes e de suas causas, cálculo dos riscos que estes perigos representam elaboração e aplicação de medidas de redução destes riscos quando necessárias, com a posterior verificação da eficiência das medidas adotadas.

A engenharia de software agrega tudo àquilo que é importante para construir um produto, mas atualmente, muitas empresas, prestadores de serviço e gestores de TI, ignoram as melhores práticas em função de tempo e custos que consideram como itens de maior prevalência nos projetos de TI.

A insatisfação de clientes não é pouca quando foram gastos milhares de dólares para investir numa solução que não atende às suas expectativas, ou que acabam tendo um desgaste muito grande devido a inúmeros fatores que acabam gerando um custo maior ou até mesmo acabam virando um problema para uma determinada instituição. A inexistência de uma boa gestão para demonstrar os riscos e construções de cenários que poderiam auxiliar a uma decisão que não comprometessem os sonhos daqueles que apostaram na TI, acreditando que ela fosse a melhor solução dos seus problemas, podem comprometer todo um trabalho de gestores de TI.

Os executivos precisam entender quais os são os riscos que podem gerar um impacto nos seus negócios e como é possível certificar que estes riscos estão sendo tratados. Cada vez mais, os gestores precisam estar conscientes dos problemas que um recurso da TI, pode afetar seus negócios, tais como o impacto de um servidor parado, de alguma falha num

processo de segurança, riscos de falhas na infraestrutura, riscos de projetos que não forem concluídos, etc.

A proposta deste artigo é mostrar que não há mais como evitar uma gestão mais completa da tecnologia da informação, onde apenas o conhecimento técnico deixa de ser o mais importante, passando agora a ser o elemento principal o gerenciamento da TI utilizando as ferramentas da qualidade, utilizando indicadores, fazendo uma análise crítica dos problemas, incorporando o gerenciamento de riscos com base no planejamento estratégico da organização.

A identificação dos riscos estratégicos compreende uma fase importante do Plano Diretor de Gestão de Riscos. A partir da fotografia, conseguida através dos cenários, identificação dos fatores críticos de sucesso e do diagnóstico estratégico, temos que identificarem quais são os perigos que podem expor os Fatores Críticos de Sucesso. Ou seja, o gestor de riscos precisa saber quais os tipos de perigos que podem prejudicar o desempenho da empresa, através de seus Fatores Críticos de Sucesso. É uma abordagem holística e estratégica, pois o gestor de riscos passa a alinhar toda sua estratégia de prevenção com a estratégia da empresa. [4]

Riscos

Um dos maiores erros dos seres humanos é confiar confiando em todas as ações e acontecimentos que os envolvem.

Numa empresa que forneça vendas de produtos pela internet, caso tenha seus serviços paralisados pela invasão ao seu site, ou se houver a quebra de um servidor ou ainda que haja problemas com o link que impeçam que seus usuários acessem o seu site. Qual o impacto deste problema para esta empresa?

Um hospital que possua, apenas, um servidor de banco de dados para atender o seu sistema de gestão hospitalar e num dado momento, o servidor apresenta algum problema que cause uma paralisação por várias horas ou dia. Qual o impacto desta paralisação para este hospital?

Se uma empresa que produz o jornal ficasse sem sistema para atender a redação, num determinado dia, qual o impacto deste problema frente ao seu negócio?

Se um servidor para, é suficiente voltar o backup do dia anterior?

E se a fita com backup do dia anterior der erro de leitura?

Como fica o vazamento de informações de salários da alta gestão de uma empresa?

Os clientes de um banco se sentiriam confortáveis ao ver seus saldos e aplicações vazadas numa mídia qualquer?

[4] Brasiliano, Antonio Celso Ribeiro , 2008

Um banco sem poder manter as suas operações bancárias por um dia, prejudicaria a sua imagem?

Existem muitas razões que podem afetar um negócio, mas podemos evitá-los ou minimizar os seus impactos, podemos contornar as catástrofes?

Afinal, existe algum espaço, em qualquer empresa, para que se possam prever situações e problemas?

Analisar um risco é identificar, discutir, e avaliar as possibilidades de ocorrência de acidentes, na tentativa de se evitar que estes aconteçam e, caso ocorram, identificar as alternativas que tornam mínimos os danos subsequentes a estes acontecimentos.

Risco pode ser definido como uma ameaça em potencial de danos e suas consequentes perdas sobre sistemas, atividades, seres e coisas. É uma expectativa de perdas e danos que coexiste com os objetos de riscos, em todos os seus ambientes. Os objetos de risco são os patrimônios e as pessoas e o nível de perda para a organização, dependerá exclusivamente do nível de proteções contra os riscos. [5]

Os riscos podem ser culposos, um risco previsível, que pode ocorrer por imprudência, negligência e imperícia e um risco doloso onde há a intenção de alguém que deseja provocar um resultado negativo para uma organização.
A análise de riscos tem por objetivo responder a perguntas como:

- Quais os prováveis riscos presentes numa empresa?
- Qual a probabilidade de ocorrência de acidentes devido a estes riscos?
- Quais os efeitos e as consequências destes acidentes?
- Como poderiam ser eliminados ou reduzidos estes riscos?

Importância da Qualidade na TI

Desde os tempos primórdios, o homem tinha como objetivo a fazer trabalhos que pudessem atingir os seus objetivos, seja com a caça, com o serviço de artesanatos,com as suas construções e até mesmo nas guerras contra os seus inimigos.

As pirâmides do Egito e as grandes obras como as gregas e romanas já demonstravam a capacidade das civilizações de desenvolver trabalhos com alta qualidade.
A Qualidade é a capacidade de qualquer objeto ou ação de corresponder ao objetivo a que se propõe.

O conceito de Qualidade foi primeiramente associado à definição de conformidade às especificações, um sinônimo de perfeição na fabricação de um produto. Posteriormente o conceito evoluiu para a visão de Satisfação do Cliente.

A satisfação do cliente não é resultado apenas e tão somente do grau de conformidade com as especificações técnicas e ausências de defeito, mas também de fatores como prazo e

[5] Almeida, Roberto Rodrigues , 1996

pontualidade de entrega, condições de pagamento, atendimento pré e pós-venda, flexibilidade, etc...

A qualidade é hoje uma das principais estratégias competitivas nas diversas empresas e nos diversos setores.

A qualidade está intimamente ligada à produtividade, a melhoria de resultados e aumento de lucros, através de redução de perdas e do desperdício, do envolvimento de todos na empresa e consequente motivação.

A qualidade deixou de ser um aspecto do produto e responsabilidade apenas de departamento específico, e passa a ser um problema da empresa, abrangendo, como tal, todos os aspectos de sua operação.

Para conquistar mercados e se manter competitivo, é preciso atender aos requisitos dos clientes quanto a produtos e serviços. Cliente insatisfeito pode resultar em má reputação, dificuldade em conquistar novos pedidos, perda de faturamento e dificuldade de se manter no negócio.
As empresas têm problemas que dificultam a obtenção de uma melhor qualidade e produtividade, e uma maior competitividade. Para a solução dos problemas é necessário a identificação da sua causa básica. A identificação da causa básica dos problemas deve ser feita através da análise dos processos, de acordo com uma sequencia de procedimentos lógicos, baseada em fatos e dados.

Para auxiliar no processo da qualidade, são utilizadas as ferramentas da qualidade que surgiram através de um conjunto de práticas que auxiliam a identificar os problemas, a analisar as causas básicas, a planejar e programar as ações corretivas para eliminar as causas, a verificar os resultados e a estabelecer controles para atingir as metas de melhorias.

Dentre as principais ferramentas, podemos destacar: Mapeamento de Processos, Diagrama de Ishikawa, Gráfico de Pareto, 5W2H, PDCA, Histogramas, etc..

Uso de Indicadores

Os indicadores são ferramentas básicas para o gerenciamento do Sistema Organizacional e as informações que fornecem são essenciais para o processo de tomada de decisão. Podem ser obtidos durante a realização de um processo ou ao seu final.

Para se fazer a medição se um processo, atividade ou tarefa estão seguindo padrões de qualidade, são utilizados indicadores de desempenho que avaliam parâmetros de tempo de execução, custos, parâmetros de qualidade, índices de perdas na produção, parâmetros de quantidade de erros na execução de tarefas, insatisfações de clientes, atendimentos, parâmetros de moral e ética na organização e para com seus clientes, parâmetros de segurança, eficiência, efetividade, eficácia, etc..

Assim sendo, os indicadores de desempenho monitoram as atividades para analisar se houve ou não o cumprimento dos objetivos previamente traçados pelo planejamento estratégico.

As Gestões de TI e as Melhores Práticas

As melhores práticas não são consideradas como uma metodologia, porque descrevem processos de alto nível sem especificamente detalhar como devem ser implantados. Entretanto, são consideradas como uma ótima base para auxiliar na elaboração de uma metodologia para a organização.

Exista uma grande quantidade de modelos de gestão de TI tratados na literatura, sendo que muitos deles incluem a gestão de riscos nos respectivos modelos. É importante ressaltar que estes modelos de gestão de TI visam a garantia da qualidade do processo na tecnologia da informação, ficando a cargo de cada organização determinar se determinada prática é a melhor ou não, e se deve ser utilizada ou não. Dentre estes modelos podemos citar:

- PMBOK / PMI
- ITIL
- COBIT
- SCRUM

ISO

A ISO (International Organization for Standardization), é uma organização não-governamental fundada em 1947, em Genebra que criou um grupo de normas técnicas que são um padrão internacional destinado para empresas que desejam implementar um sistema de gestão da qualidade e que por ser um modelo genérico,estas normas podem ser aplicadas a todas organizações, independente do setor de atuação.

Uma organização que implantou o seu sistema de gestão da qualidade baseado na ISO, pode auditá-lo e também pode optar por solicitar aos seus clientes que realizem esta auditoria, com a finalidade de garantir aos mesmos a certeza de que ela é capaz de entregar produtos e serviços que atendam aos seus requisitos. A organização pode contratar, também, os serviços de um organismo de certificação independente.

Com o objetivo de orientar a qualidade para os serviços da TI, foi desenvolvida a norma ISO 20000 que pode ser descrita como uma norma para avaliação da maturidade do Sistema de Gestão de Serviços de TI.

Já a ISO/IEC 27001 é uma norma internacional que define os requisitos para um Sistema de Gestão de Segurança da Informação, auxiliando as empresas a proteger seus ativos da informação.

Discussão

A dependência dos recursos de TI é muito acentuada em muitos países, e hoje já se integram com equipamentos industriais e hospitalares, podem ser usados para capacitar

países nas suas máquinas de guerra, podem auxiliar nos processos de cirurgias num hospital, podem controlar e movimentar maquinas, podem ser usados incorporando chips em animais e seres humanos para beneficiá-los ou controlá-los, podem controlar trens, aviões, automóveis caminhando para um processo sem um condutor, enfim cada vez mais a tecnologia vai permitir que muitos sonhos se realizem, porém se os mesmos não forem monitorados, estes benefícios poderão se tornar novos tipos de armamentos de perigo para a humanidade, poderão "quebrar" empresas, poderão alterar rotinas de uma forma indesejável, poderão expor pessoas e empresas de uma forma negativas, etc..

Grande parte dos riscos foge do controle das empresas, portanto, a única opção é ter planos para caso os riscos se tornem verdade. A importância de se analisar os riscos cresce a cada dia e a proposta é gerenciar os riscos é fazendo o uso de ferramentas e processos que possam diminuir ou evitar os riscos de algo inesperado vir a acontecer.
Neste mundo cada vez mais digital, o homem passa a ser responsável pela geração e remediação de seus próprios males.

Portanto, se torna extremamente importante para as empresas, fazer com êxito, a gestão de riscos da TI, pois ela proporciona uma correta proteção dos ativos e do patrimônio dos acionistas, eliminando ou reduzindo, efetivamente, a maioria dos riscos acidentais.

As empresas que utilizarem as referências do PMBOK, ITIL, COBIT, entre outros frameworks terão impactos minimizados, quanto aos riscos nos seus negócios, quando estes estiverem uma ligação com os recursos de TI, uma vez que a gestão de riscos já faz parte das respectivas práticas.

Numa avaliação mais ampla, a gestão de riscos deveria ter um departamento próprio numa organização e no que se refere à TI, é muito provável, que hoje esta área já merecesse um departamento de riscos exclusivo.

Para que uma empresa inicie a gestão de riscos, é essencial a aceitação dos riscos nos negócios e alinhar o quanto estes riscos podem comprometer os objetivos estratégicos da mesma. Desta forma, o gerenciamento de riscos pode conduzir de forma mais segura os rumos dos negócios da organização, fazendo com que seja possível correr riscos controlados.

Não há uma perspectiva de melhoria das empresas e crescimento profissional quando não existe a conscientização de que os processos de mudanças são necessários quando aplicado para dar uma maior segurança e efetividade nos negócios de uma organização.

Conclusão

A gestão de riscos deverá ser um processo importante e contínuo, e deverá fazer parte da estratégia das organizações, já que como sabemos os riscos de TI, não são de responsabilidade somente de TI, mas sim de toda a organização, principalmente dos tomadores de decisão.

A área da qualidade deverá ser uma referência para a área de riscos, oferecendo os processos, as ferramentas da qualidade que deverão ser usadas como linha mestra para uma

completa excelência na gestão de riscos. Não poderão faltar as auditorias que vão poder medir os andamentos dos trabalhos da gestão de riscos.

Conclui-se, portanto, que a gestão de riscos na TI é um dos grandes pilares para a sustentabilidade os negócios e desta forma não pode ser tratada como uma mera causa especifica, mas sim, como um processo ligado a todos os setores da organização, especialmente sendo planejado, executado e controlado, juntamente com os programas de qualidade da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

1. ALMEIDA, ROBERTO RODRIGUES DE. Gerência de Riscos.O Desafio. Recife.: Editora Universitária da UFPE,1996. 146p.
2. BRASILIANO, ANTONIO CELSO RIBEIRO. Fatores críticos de sucesso e a gestão de riscos. Disponível em: <http://www.brasiliano.com.br/blog/?p=312> . Publicado em 30/07/2008. Acesso em: 20/02/2012.
3. GIL, ANTONIO CARLOS. Como elaborar projetos de pesquisa. São Paulo: Atlas, 1991.
4. MAGALHÃES, IVAN LUIZIO; PINHEIRO, WALFRIDO BRITO. Gerenciamento de Serviços de TI na Prática. 2. Ed. São Paulo: Novatec, 2007. 667p.
5. MINAYO O, MARIA CECÍLIA DE SOUZA. O desafio do conhecimento. São Paulo: Hucitec, 1993.