CENTRO UNIVERSITÁRIO FEEVALE

LUIZ FELIPE SOARES PAUPERIO

PROPOSTA DE UM MODELO PARA A GESTÃO DE RISCO

Novo Hamburgo, julho de 2007.

LUIZ FELIPE SOARES PAUPERIO

PROPOSTA DE UM MODELO PARA A GESTÃO DE RISCO

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Ciência da Computação
Trabalho de Conclusão de Curso I

Professor Orientador: Roberto Scheid

Novo Hamburgo, julho de 2007.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram nesta primeira fase deste trabalho:

Aos amigos, familiares e às pessoas que convivem comigo diariamente, minha gratidão, pelo apoio emocional - nos períodos mais difíceis desta primeira etapa.

Agradeço também aos meus colegas de trabalho que entenderam minhas ausências no escritório bem como à minha namorada Juliana pela paciência durante a realização deste trabalho e ao meu professor orientador Roberto Scheid pela sua atenção dedicada.

RESUMO

A gestão da informação é essencial para a vivência de uma empresa. Gerir risco é um processo contínuo de análise e monitoração das medidas adotadas. Ferramentas atuais de gestão de informações gerenciais ainda estão deficientes na área de risco. Este trabalho tem como objetivo propor um modelo computacional para gestão de risco.

Palavras-chave: ERM. Gestão de Risco. Modelo Computacional de um Sistema de Gestão de Risco.

ABSTRACT

The management of the information are essential for the experience of a company. Risk manageament is a continuous process of analysis of the adopted measures. Current tools of information management are deficient in risk area. This work has as objective to consider a computational modeling for risk management.

Key words: ERM. Risk Manageament. Computacional Modeling of Risk Manageament.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas.
COSO	Committee of Sponsoring Organizations of the Treadway Commission.
ERM	Enterprise Risk Manageament.
ERP	Enterprise Resourse Planning.
GRE	Gestão de Risco Empresarial.
ISO	International Organization for Standardization.
PMI	Project Management Institute.
ROI	Retorno sobre o Investimento.

SUMÁRIO

INTRODUÇÃO

A Gestão de Risco Empresarial (GRE) é um mercado em ampla expansão. Gerir adequadamente os riscos de uma corporação pode deixar ela mais competitiva no mercado perante os concorrentes,além de possibilitar uma melhor qualidade em seus produtos ou processos. Estão em desenvolvimento ainda normas para auxiliar na gestão de risco: um exemplo é a norma ISO31000 com previsão de lançamento para o ano de 2009. Esta norma irá tratar de riscos em geral.

Atualmente, sistemas de gestão de informações ERP (Enterprise Resourse Planning) são muitos difundidos entre as empresas deixando as mesmas no mesmo patamar se for levado em conta a ferramenta de gestão em si. Um sistema de gestão (Diga-se SAP, Datasul, Oracle e etc...) para uma empresa é uma ferramenta essencial e talvez já não traga um ganho de competitividade o uso de uma ou outra destas ferramenta. A gestão do risco poderá ser um diferencial no processo decisório a respeito de investimentos, rentabilidade e construção do cálculo do custo. A adoção de sistemas ERM (Enterprise Risk Manageament) é uma tendência. Seja por imposição de legislações ou por requisitos para adquirir certificações (ISO, PMI) ou até mesmo para buscar uma maior competitividade no mercado. "... embora o ERM já seja conhecido no universo acadêmico da administração de empresas desde o final da década de 1990, o conceito ainda pode ser considerado uma 'tendência'no Brasil." (BASTOS, apud AMANHÃ, 2007, p.50).

No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) criou a Comissão de Estudo Especial Temporária para Gestão de Risco. Esta comissão tem por objetivo discutir e definir normas sobre o assunto. A coordenação do grupo está a cargo de Alberto Bastos, sócio fundador da Módulo, que também representa o Brasil junto ao comitê da ISO internacional.

A Gestão de Risco está em pauta no mundo dos negócios e normas que estão em desenvolvimento abrangem o assunto.

> "É comum que as empresas tratem a gestão de riscos de forma isolada e muitas vezes em feudos (ou silos), utilizando terminologia, sistemas, critérios e conceitos diferentes. Mas na visão corporativa, os riscos devem ser vistos de forma unificada! Acreditamos que depois de pronta, a ISO que terá uma adesão imediata em todo o mundo". (BASTOS, apud SETRIX, 2007)

Até 2009, deverá ser lançada a primeira versão da ISO 31000 que irá tratar das questões de gerenciamento de risco. Portanto, um sistema de ERM será uma ferramenta de fundamental importância para as empresas adequarem-se à essa nova ISO. "'É tudo feito na mão, em Word, Excel. Não há uma abordagem automatizada integrada para gestão de risco', afirma Alberto Bastos, do comitê brasileiro da ISO 31000" (BASTOS, apud AMANHÃ, 2007, p.49)

A proposta deste trabalho é desenvolver um modelo computacional de um sistema de gestão de risco (ERM) futuro visto que o mercado necessita e necessitará cada vez mais deste modelo de gestão. "Por obrigação ou não, o fato é que o gerenciamento de risco se difunde entre as companhias de todo o mundo." (BASTOS, apud AMANHÃ, 2007, p.48).

Para aprimorar o desenvolvimento da arte de gerenciar risco, o autor Apgar (2006) faz quatro recomendações:

1) Reconhecer os riscos não-aleatórios (riscos onde o aprendizado é maior);
2) Identificar os riscos não-aleatórios onde pode-se aprender mais depressa;
3) Aprender os riscos de um projeto de cada vez;
4) Ter rede de parceiros para compartilhar o aprendizado sobre riscos.

Apgar (2006) lembra ainda que o grau de incerteza é diretamente proporcional ao nosso grau de desconhecimento a respeito de um evento.

Descreve-se a seguir a estrutura da pesquisa:

- O primeiro capítulo trata dos objetivos gerais e específicos do trabalho;
- O capítulo 2 faz uma abordagem do que é risco, contempla componentes que fazem parte da gestão de risco empresarial e as vantagens que o mesmo pode trazer;
- A forma holística de gerenciamento, ou seja, a forma mais ampla de como ver a gestão de risco é tratada no capítulo 3. Este capítulo descreve também algumas ferramentas utilizadas na área de gestão;

- Alguns modelos de gestão de risco estão descritos do capítulo 4. Tais como: o COSO; a AS/NZS 4360 (norma Australiana / Neozelandesa para gerenciamento de riscos) e a ISO 31000 (ainda em desenvolvimento);
- No quinto capítulo, apresenta um sistema de gestão de riscos e suas respectivas características;
- No final deste trabalho é feita a conclusão que engloba a revisão bibliográfica realizada até o momento. Além disso sintetiza o conteúdo a ser tratado no Trabalho de Conclusão II.

1 OBJETIVOS

A seguir, descrevem-se os objetivos do trabalho a ser desenvolvido.

1.1 Objetivo geral

Propor um modelo computacional para gestão de risco.

1.2 Objetivos específicos

Esta pesquisa tem como objetivos específicos:

- Identificar, a partir do referencial teórico, os principais conceitos e/ou requisitos referentes à Gestão de Risco;
- Verificar propostas de sistemas já existentes que abordam a Gestão de Risco;
- Analisar maneiras de gerir riscos;
- Desenvolver um modelo computacional capaz de auxiliar a construção de sistema informatizado de gestão de risco.

2 GERENCIAMENTO DE RISCO

Este capítulo traz uma breve introdução sobre gerenciamento de risco.

2.1 O que é risco?

Segundo Ferreira (2002) “Risco é a probabilidade de perda ou incerteza associada ao cumprimento de um objetivo. Para cada objetivo proposto deve ser feito um processo de identificação dos riscos.”

2.2 O que gerenciamento de risco?

Baraldi (2004) diz que o gerenciamento de riscos, de oportunidades e de controles internos são os conhecimentos, os métodos e os processos organizados para reduzir os prejuízos e aumentar os benefícios na concretização dos objetivos estratégicos.

2.3 O que é gestão de risco empresarial?

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, apud SINFIC, 2007), define a gestão de risco empresarial da seguinte forma:

> "a gestão do risco empresarial é um processo realizado pelo conselho de administração, pela gestão e por outro pessoal, aplicado no ambiente estratégico e ao longo da empresa, planejado para identificar acontecimentos que possam afetar a entidade e gerir os riscos que se encontram dentro do risco aceitável, para proporcionar uma segurança razoável em relação à realização dos objetivos da entidade".

Assumindo esta explicação podemos concluir que gestão de risco empresarial é:

- Um processo (existe uma continuidade e não um início e fim);

- Realizado por pessoas (envolve toda uma organização);
- Aplicado à estratégia;
- Aplicado ao longo da empresa (em cada nível e unidade);
- Planejado para identificar potenciais eventos que afetam a organização e para gerir o risco dentro de níveis aceitáveis;
- Uma garantia para a gestão e para o conselho de administração das organizações;
- Adaptado para a realização dos objetivos.

Para a *Canadian Standards Association* Q850 (1997), gestão de riscos é definida como uma "aplicação sistemática das diretrizes sobre gerenciamento de riscos, métodos e práticas em termos de análise, avaliação, controle e transmissão de informações sobre riscos".

O gerenciamento de risco, de oportunidades e de controles internos são os conhecimentos, os métodos e os processos organizados para reduzir prejuízos e perdas e com isso ajudar a empresa a atingir seus objetivos estratégicos.

Segundo Baraldi (2004), o processo de gerenciamento dos riscos bem como de suas causas e conseqüências e a percepção de oportunidades pode ser resumido como: identificar, quantificar, selecionar e decidir (definir a atitude a ser tomada), informar e comunicar, acompanhar e aperfeiçoar de uma forma mais completa, exata e atualizada, oportuna e aprovada. Alguns riscos, bem como suas respectivas causas e conseqüências, podem interagir entre si, maximizando ou minimizando o impacto nos objetivos. Mapear esse tipo de situação é uma das funções eficientes do gerenciamento de riscos.

2.4 Componentes da Gestão do Risco Empresarial

Seguindo o conceito da SINFIC (2007), a gestão empresarial do risco consiste em componentes inter-relacionados. Isto deriva da forma como a gestão gere o negócio e está integrado com o processo de gestão. A seguir, descreve-se estes componentes.

- **Ambiente interno** - A gestão estabelece uma filosofia, considerando o risco, e estabelece um desejo de risco. O ambiente interno estabelece a fundação para a forma como o risco e os controles são vistos e tratados pelas pessoas da entidade;

- **O cenário dos objetivos** - Os objetivos devem existir antes de a gestão poder identificar eventos que afetam a sua realização. A gestão do risco empresarial assegura que a gestão tenha um processo para estabelecer objetivos de acordo com a missão e visão, e consistentes com o desejo de risco;
- **Identificação do evento** - Os eventos potenciais que podem ter impacto na entidade devem ser identificados. A identificação do evento inclui identificar fatores - internos e externos - que influenciam como os potenciais eventos podem afetar a implementação estratégica e a realização dos objetivos. Isto inclui distinguir os eventos potenciais que representam riscos - os que representam oportunidades e aqueles que representam ambos;
- **Avaliação do risco** - Riscos identificados são analisados para se determinar como devem ser geridos. Os mesmos estão associados com os objetivos relacionados que podem ser afetados. A avaliação considera a probabilidade e o impacto dos riscos;
- **Resposta ao risco** - A gestão seleciona uma abordagem ou um conjunto de ações para alinhar os riscos avaliados com o desejo de risco da entidade, no contexto da estratégia e dos objetivos. O pessoal identifica e avalia possíveis respostas ao risco, incluindo evitar, aceitar, reduzir e dividir o risco;
- **Atividades de controle** - São estabelecidas e executadas políticas e procedimentos para ajudar a assegurar que as respostas ao risco selecionadas são efetivamente aplicadas;
- **Informação e comunicação** - A informação relevante é identificada, controlada e comunicada numa forma e num período de tempo que permite às pessoas compreenderem suas responsabilidades. A informação é necessária a todos os níveis de uma entidade para identificar, avaliar e responder ao risco. A comunicação deve percorrer a entidade de cima para baixo, através e de baixo para cima;
- **Monitoramento** - Todo o processo da gestão do risco empresarial deve ser monitorado e, se necessário, proceder a modificações. Neste caso, o sistema pode reagir de forma dinâmica, mudando como as condições permitem. A monitoração é realizada através das atividades de gestão contínuas, separação das avaliações dos processos de gestão e do risco empresarial, ou de uma combinação dos dois.

A gestão do risco empresarial é um processo dinâmico. A avaliação conduz à resposta de risco e pode influenciar as atividades de controle e realçar uma necessidade para

reconsiderar os requisitos de informação e comunicação, ou atividades de monitoração da entidade. Além disso, a gestão do risco empresarial é um processo interativo e multi-direcional, no qual cada componente pode influenciar o próximo.

2.5 Vantagens da Gestão de Risco Empresarial

A SINFIC (2007) coloca como exemplo algumas vantagens que a gestão de risco proporciona para as empresas. A gestão do risco empresarial proporciona às organizações uma melhoria da sua capacidade para:

- **Alinhar o risco aceitável com a estratégia organizacional.** O risco aceitável é o grau de risco que uma organização está disposta a aceitar na busca dos seus objetivos. A gestão considera o risco aceitável para a avaliação de estratégias alternativas e depois alinha os objetivos com a estratégia adotada, desenvolvendo mecanismos para gerir os riscos relacionados;
- **Aumentar a capacidade de gerir o risco e otimizar o retorno.** A GRE proporciona uma melhoria da capacidade para identificar e avaliar os riscos, aumentando o retorno;
- **Melhorar as decisões de resposta aos riscos.** A gestão do risco empresarial proporciona rigor para identificar e selecionar as respostas alternativas ao risco - anulação, redução, partilha e aceitação do risco. A gestão do risco empresarial proporciona metodologias e técnicas para a tomada de decisões;
- **Minimizar as surpresas operacionais e os prejuízos.** A gestão do risco permite melhorar a capacidade das organizações para identificar potenciais eventos, avaliar os riscos e estabelecer respostas, reduzindo deste modo a ocorrência de surpresas e a sua relação com custos ou perdas;
- **Identificar e gerir os riscos transversais às organizações.** Cada entidade enfrenta uma miríade de riscos que afeta diferentes partes da organização. A gestão precisa assim de gerir os riscos individualmente e de compreender os impactos inter-relacionados;
- **Proporcionar uma resposta integrada para múltiplos riscos.** Os processos de negócio têm muitos riscos inerentes e a GRE permite integrar soluções para gerir os riscos;

- **Aproveitar as oportunidades.** A gestão considera eventos potenciais, mais do que riscos. Ao considerar um conjunto completo de eventos, a gestão obtém uma compreensão de como certos eventos representam oportunidades;
- **Racionalizar o capital.** A disponibilidade de mais informação sobre os riscos permite uma gestão mais eficaz da avaliação das necessidades de capital e melhora a distribuição do mesmo.

3 GERENCIAMENTO HOLÍSTICO DO RISCO

Abaixo segue uma forma diferenciada de gerenciamento e também como define Schneier (1998) “... essa estratégia não-convencional envolve a avaliação e a conformação do risco em todo o negócio”.

Schneier (1998) assume que quase todos os dias os jornais trazem notícias sobre o sério impacto e conseqüências que frustram as expectativa de investidores, como uma empresa que viu suas ações caírem mesmo tendo um grande aumento de lucros. Somem-se a isso as exigências de regulamentação e controle e fica evidente por que o risco é tão importante para os altos executivos das empresas. Afinal, é a eles que cabe gerenciar os riscos do negócio, e o não cumprimento desse preceito é uma quebra da responsabilidade confiada.

Mesmo que os lucros e os preços das ações sejam saudáveis, a obtenção de resultados atualmente é bem mais arriscada que no passado. O motivo deste acontecimento se dá devido a maioria dos negócios estar de forma globalizada. Nesse âmbito expandindo, traz maiores oportunidades, mas também maior complexidade. “O aumento da complexidade, por sua vez, traz um potencial maior de as coisas darem errado.” (Schneier, 1998)

3.1 A gestão do risco e as ações

A maioria das decisões envolve uma escolha entre algum tipo de risco e a sua recompensa a ele associada.

> "Cria-se um valor para o acionista quando a recompensa excede o custo do risco. O custo do capital é uma taxa genérica que reflete o risco de determinada classe de investimento. Se a recompensa (ROI – Retorno sobre o Investimento) foi maior que essa taxa, o investimento vale proporcionalmente mais." (Schneir , 1998)

3.2 Tipos de riscos e gerenciamento

Risco é a possibilidade de alguma coisa dar errado e fatores de risco são as condições que dão origem a essa possibilidade. O risco é um resultado, não algo que se possa gerenciar diretamente. Os fatores de risco, como causas, sim. Ao gerenciar o risco, a maioria das empresas presta atenção ao resultado e não à causa do mesmo e acaba por errar.

Schneier (1998) compreende que a abordagem padrão é concentrar-se no financiamento do risco, provisionando recursos para atenuar a variabilidade de receita de riscos não controlados. A idéia básica é que algum risco financeiro, por exemplo, tem uma possibilidade razoável de ocorrer. Como não se pode fazer nada para impedi-lo, os executivos deveriam separar uma quantia para pagar os danos deste problema gerado.

Este tipo de abordagem tem um problema segundo Schneier (1998) por não tratar o risco de forma “pró-ativa”.

3.3 A abordagem holística

Diante deste tipo de gerenciamento, chega ao mercado um novo conceito de gestão para os gestores de empreendimentos: o gerenciamento holístico do risco. As técnicas de gerenciamento holístico do risco têm sido uma ferramenta poderosa para o gerenciamento em várias empresas, quando aplicadas corretamente.

O ERM aborda os principais riscos da companhia em um determinado nível do empreendimento. “a prática do ERM varia, pois cada empresa é singular do ponto de vista de riscos.” (Schneier, 1998)

O GRE é uma abordagem sistemática segundo a qual os fatores de riscos e os programas de atenuação são considerados ao negócio como um todo, interna e externamente. Admite também que os fatores de risco possuem efeitos múltiplos e, para terem algum valor, os programas de atenuação devem considerar todos esses efeitos.

O modelo ERM é “pró-ativo” e com isso a primeira linha de defesa contra o risco é “conformá-lo”, que significa controlá-lo por meio do comportamento organizacional.

> "Quando corretamente implantado, o ERM exige trabalho árduo e comprometimento da alta gerência. Entretanto, para companhias que praticam o ERM com eficácia, as recompenças podem ser a liderança de mercado, crescimento contínuo, elevação nos preços das ações e confiança dos investidores." (Schneir, 1998)

Uma maneira de verificar se o ERM está sendo implantado com eficácia é determinar se os fatores de risco da empresa se parecem com os de suas concorrentes. Em caso positivo, ou se eles não mudarem à medida que a organização e seu ambiente operacional mudarem, é provável que esses riscos estejam definidos de forma muito genérica.

Conforme Schneier (1998), os riscos gerenciáveis são os que na exigem são os que não exigem investimento significativo e podem ser abordados na condução normal dos negócios. Os riscos estratégicos, por outro lado, talvez necessitem um investimento razoável de capital ou mudança de rumo.

3.4 Quantificação dos riscos e limiares

A quantificação dos fatores e dos limiares de risco é necessária para o perfeito funcionamento do ERM. Schneier (1998) completa: “Há vários modelos e metodologias, alguns mais acessíveis, outros mais complexos. Com um pouco de criatividade, os gerentes conseguem quantificar os fatores de risco de forma rápida e fácil.”.

3.5 Um guia para ERM

A adoção de práticas de ERM exige comprometimento e um nível razoável de esforço em suas fases principais. Descreve-se agora um guia do tipo “faça-você-mesmo” adaptado de Schneier (1998).

3.5.1 Fase 1: avaliação do risco

O objetivo da avaliação é identificar, priorizar e agregar todos os riscos com que a companhia depara. Os passos desta fase são:

- **Revisão da infra-estrutura.** A empresa começa por uma revisão sistemática da infra-estrutura, dos processos decisórios e dos sistemas. Identifica as preocupações da gerência por entrevistas e verifica-las a partir de dados externos. Procura um acordo quanto a um meio de medir o desempenho;

- **Avaliação qualitativa do limiar do risco.** O risco, não se pode esquecer, é tanto subjetivo quanto objetivo;

- **Definição preliminar do risco.** A empresa reduz e sintetiza os dados de desempenho e do limiar do risco em um conjunto preliminar de riscos, que deve ser validado e classificado;

- **Quantificação preliminar.** Em geral, é aconselhável que a empresa use um modelo tipo "criação de valor para o acionista" para testar as sensibilidades e identificar fatores de risco. Então, a empresa deve checar os resultados, cruzando-os com um ou vários métodos subjetivos de avaliação. Se tiverem tido identificados fatores de risco prospectivos, ela precisa determinar o meio mais apropriado de aferição;

- **Priorização do risco.** Aqui se priorizam fatores de risco com base na probabilidade de acontecerem, no valor presente de suas conseqüências e na qualidade dos controles já em funcionamento. A empresa identifica as interações entre os fatores de risco de alta prioridade e suas conseqüências comuns. Entre as áreas nas quais vale a pena se concentrar estão comportamento e atitudes da organização, capitais empregados no negócio (de mercado, infra-estrutura, humano, financeiro) e principais indicadores de desempenho da companhia;

- **Delineamento de estratégia.** A essa altura já deve haver uma lista abrangente dos fatores de risco de alta prioridade e compreensão de suas conseqüências. Se houver acordo quanto às prioridades, a empresa delineia as estratégias gerais para atenuação.

As companhias deparam-se com a lista de fatores de risco de alta prioridade gerada na fase de avaliação, Esses fatores muitas vezes diferem daqueles nos quais os gerentes tradicionalmente concentram sua atenção.

3.5.2 Fase 2: conformação do risco

Antes dos gerentes estarem prontos para delinear os programas de conformação, eles necessitam de uma medida mais sólida dos fatores de risco. Precisam também de uma

adequada compreensão de como funciona a organização e como mudar os comportamentos. Nesta fase, os passos consistem em:

- **Modelagem dos indicadores** para medir o impacto individual e coletivo dos fatores de risco para com a empresa;

- **Quantificação do risco.** A empresa descobre as interdependências entre os fatores de risco e avalia o impacto de cada cenário na organização como um todo. O grupo gerencial deve revisar isso e chegar a um consenso sobre o que acredita ser o cenário mais provável. A empresa calcula então a exposição geral a riscos ao mesmo tempo em que se cruza a razoabilidade dos dados com as avaliações qualitativas feitas na fase de avaliação;

- **Mudança organizacional.** Dentro do cenário que se determinou como mais provável, talvez seja preciso projetar programas para mudar o comportamento. Em alguns casos, pode-se atenuar os fatores de risco ao fazer mudanças operacionais bem diretas. Em outros casos, é preciso desenvolver estratégias para reformular o comportamento dos funcionários, as capacidades da organização e a cultura;

- **Financiamento do risco.** Aqui, a empresa deve determinar se os programas escolhidos atenuarão suficientemente os riscos da companhia. Em caso negativo, é preciso projetar um programa para financiar parte do risco ou ignorá-lo. Como outros aspectos do ERM, o financiamento de risco deve ser visto de forma holística. Primeiramente a empresa determina a exposição (relativa ao limiar de risco) e após isso, a aplicação dos programas de atenuação.

3.6 Um guia para o risco estratégico

As empresas sofrem com uma série singular de riscos estratégicos fundados em fatores como o setor, posição competitiva, fontes de receita e lucro e pontos fortes da marca. Para mitigar tais riscos, é preciso identificá-los, avalia-los e reagir a eles de modo sistemático. Segue um guia adaptado de Slywotzky (2005) para identificar e tratar o risco estratégico.

- **Identificar e avaliar os riscos e avaliar os mesmos** quanto:

    - **Gravidade –** Em quanto o risco afeta a estratégia do negócio. Devem ser avaliados eventos analógicos ocorridos no setor ou em outros setores, também em fatores específicos ao negócio capazes de aumentar ou reduzir o impacto do risco;
    - **Probabilidade –** Qual a probabilidade do risco se materializar. Verificar casos anteriores em que a empresa já foi afetada pelo risco e de outras fontes externas também;
    - **Timing –** Se é possível determinar em que época é mais provável que o risco ocorra;
    - **Mudança da probabilidade com o tempo –** Verificar se a chance do evento ocorrer esta subindo, caindo ou se é uma constante. A tendência de um risco ocorrer, quando bem gerenciado, é de cair com o tempo.

- **Mapear os riscos.** Depois de identificar e avaliar os principais riscos deve-se fazer um mapa com eles para que se obtenha uma visão global da situação atual;

- **Quantificar os riscos.** Medir os mesmos de modo amplo com um critério único para que se possa comparar e consolidar os riscos e assim vinculá-los a decisões;

- **Identificar o lado bom do potencial de cada risco.** O risco pode se tornar uma oportunidade dependendo do envolvimento e a maneira como ele é gerido. A empresa pode montar um plano para identificar e maximizar o lado bom de cada item listado no mapa de riscos estratégicos;

- **Desenvolver planos de ação para mitigar riscos.** Para cada grande risco identificado, deve haver uma equipe responsável por elaborar um plano formal para mitigar tal risco. Esse documento sintetiza a avaliação do risco feito em passos anteriores;

- **Ajustar adequadamente as decisões.** Depois de elaborado um perfil explícito dos riscos que enfrenta, a empresa pode mudar seus planos para gerir o risco.

Segue um exemplo de mapa de riscos estratégicos.

Tabela 1: Exemplo de mapa de risco estratégico.

Tipo de risco	Gravidade (% do lucro em jogo)	Probabilidade	Timing esperado em anos					Mudança da probalilidade com o tempo
			1	2	3	4	5	
Tecnologia								
Mudança em tecnologia	60%	20%		x	x			Crescente
Vencimento de Patente	10%	100%					x	Constante
Marca								
Erosão	40%	20%	x					Crescente
Colapso	70%	10%	x	x	x	x	x	Constante

.

Fonte: Adaptado de Slywotzky (2005).

Com a análise do risco e com seu mapa de riscos estratégicos, tem-se uma visão ampliada do impacto e com isso pode-se traçar metas de contramedidas e criar um mapa de medidas preventivas (tabela 2):

Tabela 2: Exemplo de mapa de medidas preventivas.

Risco Estratégico	**Contramedida**
Mudança Tecnológica	Aposta dupla
Erosão da marca	Redefinir escopo de investimentos na marca Realocar investimentos na marca

Fonte: Adaptado de Slywotzky (2005).

3.7 Ferramentas e metodologias que auxiliam no processo de gestão

Existem diversas metodologias que podem auxiliar no processo de gestão e avaliação. Dentre elas, é citado a ferramenta 5W2H e o modelo PDCA. Estas farão parte do modelo computacional proposto por este trabalho.

3.7.1 A ferramenta 5W2H

A ferramenta 5W2H pode ser usada para verificação e acompanhamento dos planos de ações no que tange: O Que? *(What),* Quem? *(Who),* Onde? *(Where),* Porque *(Why),* Quando? *(Where),* Como? *(How) e* Quanto? **(**How much). Estas "perguntas" visam direcionar, planejar, definir as responsabilidades e qualificar as ações.

A tabela 3 ilustra um modelo usado na 5W2H.

Tabela 3: Modelo de tabela 5W2H

5W 2H								
Variáveis	Ações	What (O que)	Who (Quem)	Where (Onde)	Why (Por que)	Whem (Quando)	How (Como)	How much (Quanto)
Variável 1	Ação 1							
Variável 2	Ação 2							
Variável 3	Ação 1							
Variável 4	Ação 1							
Variável 5	Ação 1							

Fonte: O autor.

3.7.2 O ciclo PDCA

O ciclo PDCA tem por princípio tornarem mais claros e ágeis os processos envolvidos na execução da gestão.

Sousa comenta o início deste principio como:

> "O conceito de Métodos de Melhorias, conhecido atualmente pela sigla PDCA, foi originalmente desenvolvido na década de trinta, nos laboratórios da *Bell Laboratories* – EUA, pelo estatístico americano *Walter A. Shewart*, como sendo um ciclo de

> controle estatístico do processo, que pode ser repetido continuamente sobre qualquer processo ou problema. Em 1931, Shewart publica o livro *Economic Controlo f Quality of Manufactured Product*, o qual fornece um caráter científico às questões relacionadas à qualidade ." (SOUZA,apud ANDRADE, 2003)

Deming caracteriza que:

> "...este método somente foi popularizado na década de cinqüenta pelo especialista de qualidade W. Edwards Deming, ficando mundialmente conhecido ao aplicar este método nos conceitos de qualidade em trabalhos desenvolvidos no Japão ." (DEMING, apud ANDRADE, 2003)

Começa pelo planejamento, em seguida, a ação ou conjunto de ações planejadas são executadas. Checa-se o que foi feito, verificando se estava de acordo com o planejado, constantemente e toma-se uma ação para eliminar ou ao menos reduzir defeitos no processo ou evento.

Os passos são os seguintes:

- **Plan** (planeamento): estabelecer missão, visão, objetivos (metas), procedimentos e processos (metodologias) necessários para atingir os resultados;
- **Do** (execução): realizar e executar as atividades;
- **Check** (verificação): monitorar e avaliar periodicamente os resultados, avaliar processos e resultados, confrontando-os com o planejado, verificando objetivos, especificações e estado desejado, consolidando as informações, eventualmente confeccionando relatórios;
- **Act** (agir): Agir de acordo com o avaliado e de acordo com os relatórios, eventualmente determinar e confeccionar novos planos de ação, de forma a melhorar a qualidade, eficiência e eficácia, aprimorando a execução e corrigindo eventuais falhas.

O ciclo PDCA segue o padrão de utilização onde pode ser perfeitamente notado quem não existe um final (figura 1).

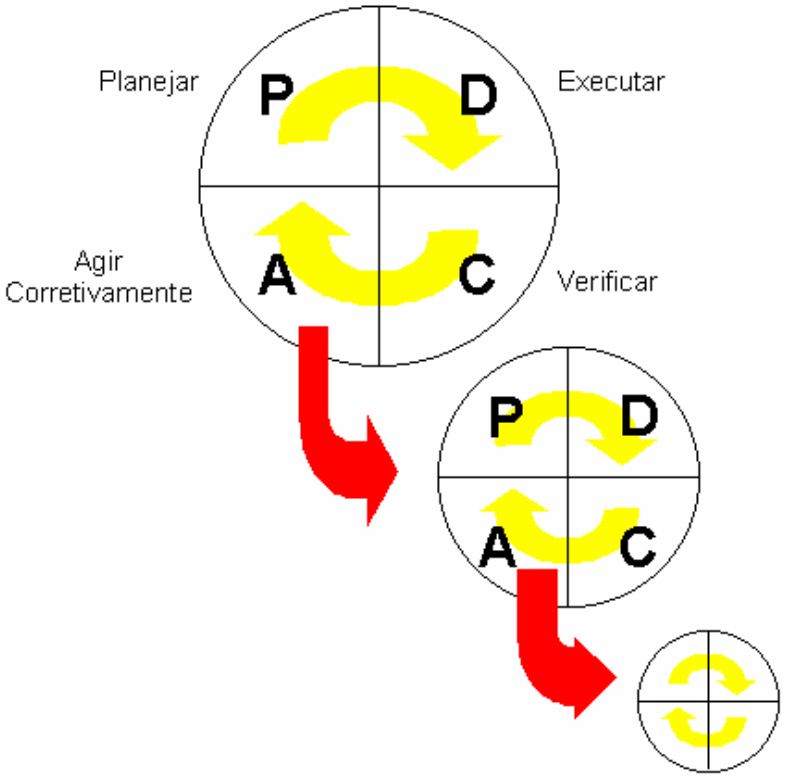

Figura 1 – O ciclo PDCA.

Fonte: Corrêa (2007).

O ciclo PDCA têm como por objetivo demonstrar como será uma das metodologias de avaliação a ser utilizada no modelo computacional proposto. A geração de um histórico de ocorrências e o acesso aos resultados das medidas adotadas anteriormente facilitam a gestão do risco. Uma abordagem de contínua observação dos resultados melhora o desenvolvimento de novas medidas corretivas a serem tomadas num processo que é cíclico (Feedback).

4 MODELOS DE GERENCIAMENTO DE RISCO

Neste capítulo está descrito alguns modelos de gestão de risco.Quais são: o COSO, a AS/NZS 4360:2004, e a ISO 31000.

4.1 História do COSO

Conforme o SINFIC (2007) , COSO pode ser definido como:

> "O COSO é a sigla do Committee of Sponsoring Organizations of the Treadway Commission e foi formado originalmente em 1985 para apoiar a National Commission on Fraudulent Financial Reporting, uma iniciativa privada destinada a estudar os aspectos que podem conduzir a relatórios financeiros fraudulentos. Paralelamente, desenvolveu recomendações para vários tipos de organizações, incluindo as organizações públicas e os seus auditores independentes, ou as instituições educacionais. Esta comissão nacional foi apoiada por grandes associações profissionais dos Estados Unidos, nomeadamente a American Accounting Association, a American Institute of Certified Public Accountants, a Financial Executives International, o Institute of Internal Auditors, ou a National Association of Accountants (actual Institute of Management Accountants)."

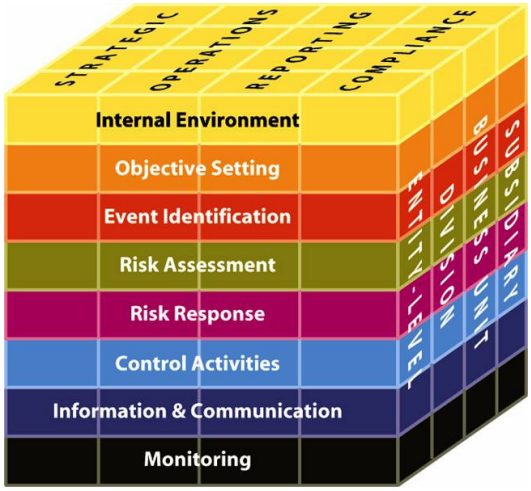

Figura 2 – O cubo COSO.

Fonte: SGIR (2007).

A figura 2 apresenta o cubo COSO. Nas atividades de definição dos objetivos, identificação dos eventos, análise e avaliação dos riscos, resposta aos riscos, controle, informação e comunicação, e acompanhamento e avaliação, as organizações precisam de ter em conta a estrutura (entidades, departamentos, unidades de negócio e a organização) e os objetivos (estratégicos, operacionais, de monitoração e de conformidade) organizacionais.

Algumas normas surgiram utilizando o modelo do cubo COSO de gestão, tais como a norma Australiana / Neozelandesa para gerenciamento de riscos.

4.2 AS/NZS 4360:2004

Na opinião de Ferreira (2006), AS/NZS 4360 é uma norma Australiana / Neozelandesa para gerenciamento de riscos que foi elaborada pela *Standards Austrália e Standards New Zealand* através do Comitê de gestão de riscos. É uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza (figura 3).

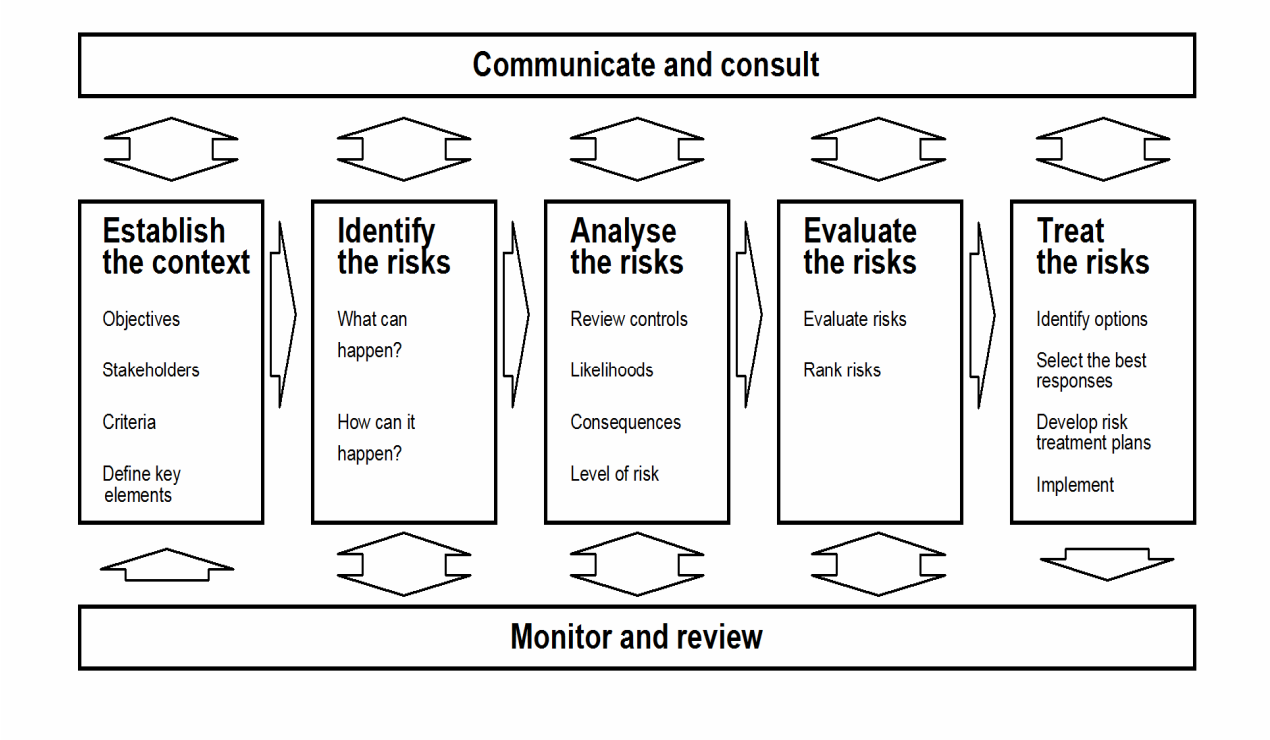

Figura 3 - Diagrama da norma AS/NZS 4360:2004.

Fonte: Standards (2007).

A figura 4 traz um detalhamento maior do processo de gestão de risco na norma.

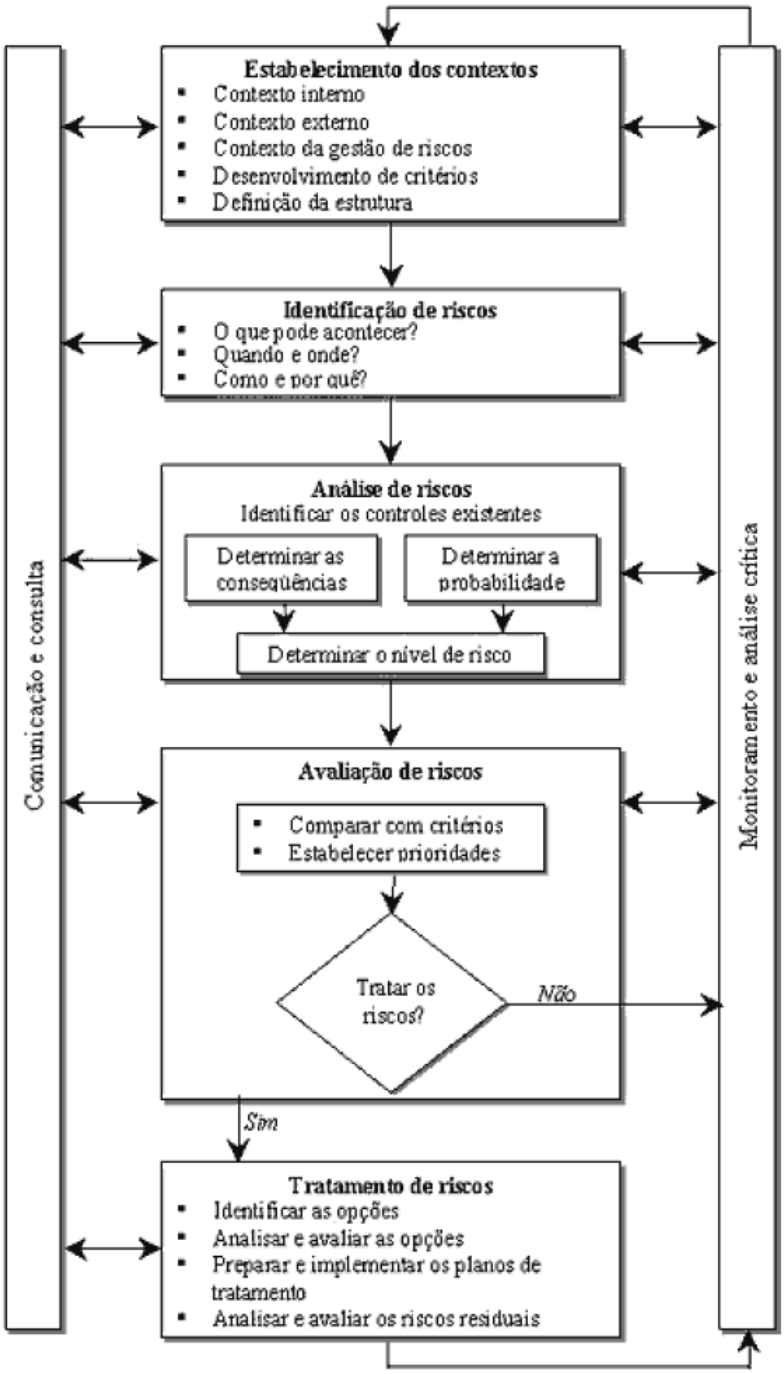

Figura 4 - Detalhamento do processo de gestão de risco proposta na AS/NZS 4360.

Fonte Modulo (2007).

4.2.1 Principais etapas da norma AS/NZS 4360:2004

Segundo a Módulo (2007), as principais etapas na norma australiana são:

- **Comunicação e consulta -** comunicar e consultar as partes envolvidas internas e externas, conforme apropriado, em cada etapa do processo de gestão de riscos e em relação ao processo como um todo;
- **Estabelecimento dos contextos -** estabelecer os contextos externo, interno e da gestão de riscos nos quais se desenvolverá o restante do processo. Devem ser estabelecidos os critérios em relação aos quais os riscos serão avaliados e deve ser definida a estrutura da análise;
- **Identificação de riscos -** identificar onde, quando, por que e como os eventos podem impedir, atrapalhar, atrasar ou melhorar a consecução dos objetivos;
- **Análise de riscos -** identificar a avaliar os controles existentes. Determinar as conseqüências e a probabilidade e, por conseguinte, o nível de risco. Tal análise deve considerar as diversas conseqüências potenciais e como elas podem ocorrer;
- **Avaliação de riscos -** comparar os níveis de risco estimados com os critérios estabelecidos previamente e considerar o balanço entre os benefícios potenciais e os resultados adversos. Isso possibilita que sejam tomadas decisões quanto à extensão e à natureza dos tratamentos necessários e quanto às prioridades;
- **Tratamento de riscos -** desenvolver e implementar estratégias e planos de ação específicos e econômicos, para aumentar os benefícios potenciais e reduzir os custos potenciais;
- **Monitoramento e análise crítica -** é necessário monitorar a eficácia de todas as etapas do processo de gestão de riscos. Isso é importante para a melhoria contínua.

4.3 A ISO 3100

Bastos (2007) cita que até 2009, deve ser lançada a primeira versão da ISO 31000, que vai tratar das questões de gerenciamento de risco. O grupo de brasileiros já contribuiu com um modelo de processo de tomada de decisão em gerenciamento de risco. Bastos informa também que, antes de norma internacional ser publicada, deve sair a homologação da ISO brasileira. O objetivo é possibilitar que as empresas possam se atualizar mais depressa quando a ISO internacional chegar.

Na opinião de Amanhã (2007):

> "A 31000 é desenvolvida com base na NS/AS 4360, norma de gestão de risco utilizada na Austrália e na Nova Zelândia e considerada a mais eficiente. Nesse documento, o risco é definido como "tudo aquilo que desvia do objetivo". Na opinião de Bastos, esse conceito é o que amarra o gerenciamento de risco às metas estratégicas de uma organização. Outro objetivo da ISO 31000 é oferecer modelos de gestão integrada do risco de forma que os diferentes setores de uma empresa possam falar "a mesma língua" ao tratar do assunto. "A idéia é que o principal executivo tenha uma visão holística dos riscos para tomar decisões mais precisas", avalia Bastos. Para isso, a ISO 31000 deverá ser aplicada em todas as áreas da empresa, de forma integral e integrada."

5 ANÁLISE DE REQUISITOS MÍNIMOS PARA UM SISTEMA DE GESTÃO DE RISCO

Pressman (1995) define que a análise de requisitos é o primeiro passo técnico do processo de engenharia de software. Aponta ainda que é nesse ponto que uma declaração geral do escopo do software é aprimorada numa especificação concreta que torna-se a base para todas as atividades de engenharia de software que irão compor o projeto.

Na opinião de Pressman (1995) a Especificação de Requisitos de Software é desenvolvida como uma conseqüência da análise, descrevendo ainda que, "A análise deve concentrar-se nos domínios funcionais, comportamentais e de informação de um problema."

As atividades de análise concentram-se na identificação, especificação e descrição dos requisitos do sistema de *software*. Em resumo, requisito é uma necessidade que o *software* deve cumprir.

Esta análise tem por objetivo levantar os requisitos –a partir da revisão bibliográfica - a ser previstos na modelagem proposta por este trabalho.

Após extensa pesquisa, verifica-se que algumas características são desejadas em um sistema de gestão de risco que seja capaz de gerir riscos de diversas naturezas:

- Possibilidade de criar contas de usuários para que o sistema possa diferenciar cada pessoa da organização dentro do sistema de gestão de risco. Estes usuários devem ser cadastrados de forma que informe o setor onde o mesmo atua bem como sua função para que possa ter um parâmetro de quem é esta pessoa. Por exemplo: vendas, gerência operacional, gerência de Ti, operação, diretoria, expedição, etc;

- Disponibilidade para que o usuário do sistema possa gerar métricas. Cada empresa tem seus riscos próprios e maneiras diversas de mensuração dos mesmos, então é importante que o sistema possua uma maneira do cliente criar e propor peso a sua

métrica. A geração de métricas têm como função colocar um peso ou outra forma de medida à um parâmetro de forma que ele possa ser medido e avaliado junto à outros quesitos;

- Banco de dados para futuras consultas. Visto que a gestão de risco é um processo contínuo (PDCA), é importante que o modelo do software preveja um repositório de dados para futuras consultas bem como para geração de indicadores. Os valores dos mesmos facilitarão a compreensão do risco e a avaliação das medidas tomadas. Tendo-se um histórico de ocorrências, a rastreabilidade de uma medida adotada tem grande valia para uma próxima decisão (possibilitando, inclusive, o aumento do índice de confiabilidade da mesma);

- Possuir um relatório com o(s) resultado(s) depois de aplicado valores para as métricas do sistema a fim de nortear futuras decisões;

- Englobar a ferramenta 5W2H. A utilização desta ferramenta pode contribuir muito para facilitar na avaliação dos quesitos para a gestão de riscos. A mesma adiciona a um banco de dados as informações básicas dos quesitos levantados tais como: o que, quem, onde, por que, quando, como, quanto;

- Utilizar o modelo PDCA para melhoria contínua dos processos de Gestão de Risco..

6 ANÁLISE DE UM SISTEMA PARA GESTÃO DE RISCO

Em pesquisa nos desenvolvedores de softwares que trabalham com sistemas de gestão de risco, nota-se que a grande maioria dos softwares são específicos para o mercado financeiro, o que não é o foco deste trabalho. Os softwares que não são voltados para o mercado financeiro não dispõem de métricas pré-definidas, mas, disponibiliza ao usuário ferramentas para criar suas próprias métricas, pesos e área empregada. Os sistemas existentes de gestão de risco possuem também um gerador de relatórios e um banco de dados para futuras consultas.

Na busca de ferramentas de gestão de risco que contribuísse com os objetivos deste trabalho, encontrou-se disponível para avaliação somente o sistema desenvolvido pela empresa Modulo.

6.1 Sistema de gestão de risco da Modulo

A Modulo é uma empresa (www.modulo.com.br) focada, entre outras atividades, no desenvolvimento de softwares para a área de risco. Modulo Risk Manager é um software da Modulo que contêm características que o deixa capaz de gerir não somente riscos financeiros, mas, riscos diversos.

6.1.1 Características do software

Uma vez que o acesso ao sistema é limitado, as seguintes características foram observadas:

- Dispõe de algumas métricas para o mercado financeiro;
- Utiliza o método de questionário para o preenchimento de campos;

- Disponibiliza para que os usuários criem suas próprias métricas;
- Possui um banco de dados (histórico) para consultas futuras;
- Contém um gerador de relatórios que pode ser configurado pelo usuário;
- Encaminha a entrevista via WEB para o usuário credenciado a responder o mesmo;
- Nas entrevistas pode se inserir comentários para futuras consultas;
- Traz um gerador de um painel com indicadores de risco, Risk Scorecard;
- Pode ser atualizado via web.

6.1.2 Imagem do sistema Modulo Risk Manager

Na figura 5, apresenta-se uma imagem do sistema.

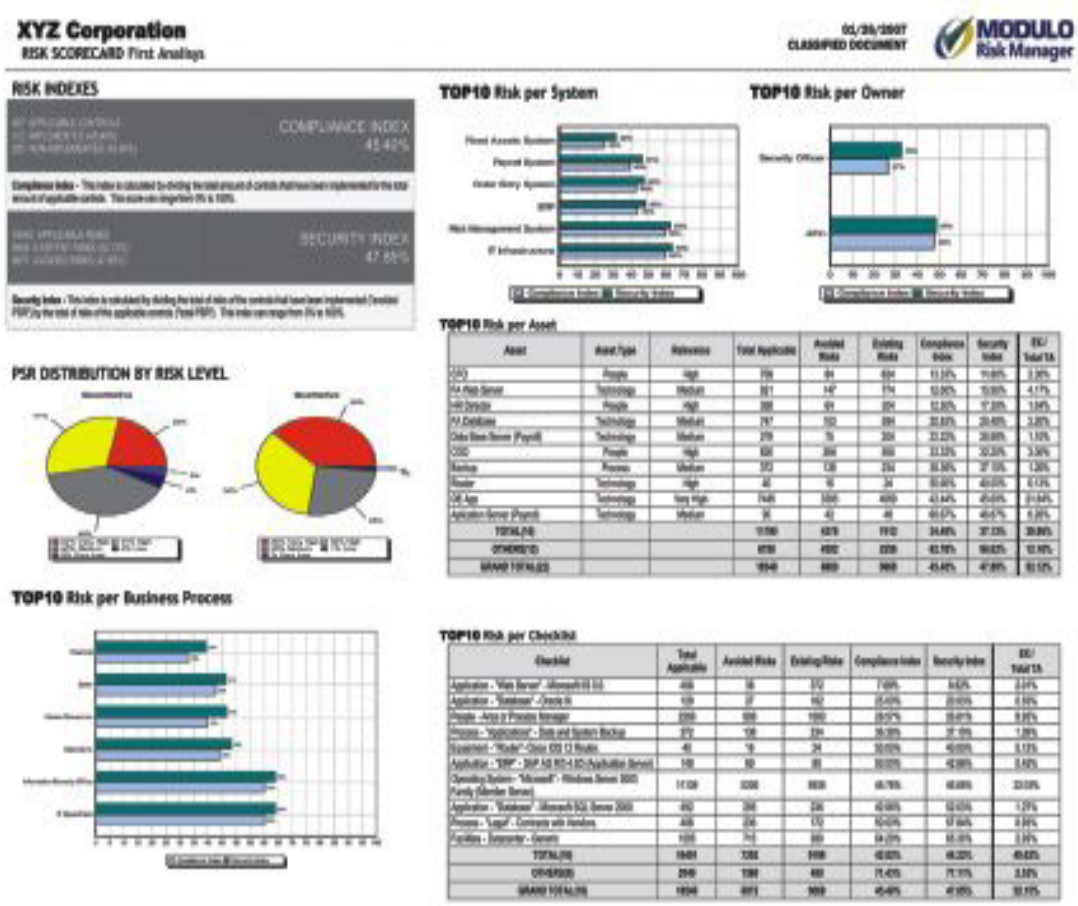

Figura 5 – Sistema - Painel de Controle e Risk Scorecard.

Fonte: Modulo (2007).

A avaliação foi limitada em função das informações disponibilizadas pela empresa em questão.

CONSIDERAÇÕES FINAIS

Esta primeira fase do trabalho de conclusão de curso teve como diretriz realizar um estudo sobre gestão de risco e as técnicas utilizadas para tal.

Verifica-se uma tendência mundial das empresas almejarem formas de se tornarem cada vez mais competitivas. Uma destas formas é a de gerir seus riscos.

Até 2009, deverá ser lançada a primeira versão da ISO 31000 que vai tratar das questões de gerenciamento de risco. Bastos (BASTOS, apud AMANHÃ, 2007, p.47) afirma que um dos objetivos da ISO 31000 é oferecer modelos de gestão integrada do risco que atuará em todos os setores da empresa. “A idéia é que o principal executivo tenha uma visão holística dos riscos para tomar decisões mais precisas..”(BASTOS, apud AMANHÃ, 2007, p.47)

A GRE permite ao executivo passar da defesa ao ataque. A busca do crescimento exige que a empresa assuma riscos e invista em certos produtos, canais, segmentos de clientes e modelos de negócios novos. A gestão do risco, além de limitar o lado ruim do mesmo, ajuda a empresa a aumentar as chances de sucesso desses investimentos, obrigando-as a pensar no futuro de modo mais sistemático.

Com base na revisão bibliográfica, projeta-se para o TC II o desenvolvimento de um modelo computacional que possa prever as necessidades que um sistema de gestão de risco deve conter. A GRE é uma tendência crescente no mundo atual.

O mercado necessitará cada vez mais de sistemáticas para a gestão dos impactos e das oportunidades. Aprender com os acertos e/ou erros do passado para avaliar a situação atual e futura poderá ser de grande valia para as corporações.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Fabio Felippe de. **O método de melhorias PDCA.** 2003. 169p Dissertação (mestrado) Escola Politécnoda, Universidade de São Paulo. São Paulo , 2003.

APGAR, David. **Risk Intelligence**: learning to manage what we don,t know. 1. ed. EUA, HBS Press Book, 2006. 224p.

BARALDI, Paulo. **Gerenciamento de riscos**: a gestão de oportunidades, a avaliação de riscos e a criação de controles internos nas decisões empresariais. Rio de Janeiro, Elsevier, 2004. 238p.

CORRÊA, Sílvio. **Ferramentas para o telegestor**: Disponível em: < http://www.widebiz.com.br/gente/silvio/telegestor.html>. Acesso em: 10 junho 2007.

FERREIRA, Luiz Eduardo Alves. **Entendendo o COSO** Disponível em: < http://www.auditoriainterna.com.br/coso.htm>. Acesso em: 15 maio 2007.

LOREA, Eduardo; GRACIANI, Marcos. Gestão: **Revista Amanhã**. p. 46-53 Porto Alegre, março 2007

MODULO, **Controles internos**: buscando a solução adequada. Disponível em: < http://www.moduloriskmanager.com.br/artigo_06.htm>. Acesso em: 11 maio 2007.

PRESMAN, Roger S. **Engenharia de software**. São Paulo, Paerson Education do Brasil, 1995. 1056p.

SCHNEIER, Robert; MICCOLIS, Jerry. Gerenciamento Holístico do Risco: **HSM Management**. p. 124-131 São Paulo, outubro 1998

SETRIX Business Continuity. **Gestão de Risco**: Brasil encara em 2007 desafio de juntar esforços para unificar normas e padrões. Disponível em: < http://www.setrix.com.br/noticia.php?cdnoticia=64>. Acesso em: 04 de abril de 2007.

SGIR: **Enterprise Risk Management Framework**. Disponível em: < http://www.clarify.com.br/sgir/metodologia_erm.asp>. Acesso em: 10 maio 2007

SINFIC, **O COSO e a gestão de risco empresarial.** Disponível em: < http://www.sinfic.pt/SinficWeb/conteudo/displayconteudo.do2?numero=22583>. Acesso em: 16 maio 2007.

SLYWOTZKY Adrian J.; DRZIK, John. Contra-atacando: o maior de todos os riscos. **Harvard Business Review**. p. 56-66 São Paulo, abril 2005.

STANDARDS, Austrália. **New Australian Standard for Risk Management**. Disponível em:<http://www.riskmanagement.com.au/News/NewAustralianStandardforRiskManagement/tabid/152/Default.aspx>. Acesso em: 11 maio 2007