



Gerenciamento de Risco

Nome do Professor: D. Sc. Cássio Aurélio Suski

1

OBJETIVOS

- ▶ Apresentar e analisar de forma crítica os princípios básicos de gerenciamento de risco, as etapas de gestão e a avaliação de riscos, bem como a aplicação das ferramentas e técnicas para redução dos riscos de forma planejada;
- ▶ Avaliar economicamente os riscos e simular os cenários econômicos de risco;
- ▶ Possibilitar o gerenciamento de processos de risco e otimização dos mesmos através da pró-atividade.

Sumário

INTRODUÇÃO	2
CONCEITOS BÁSICOS.....	2
Riscos.....	5
TIPOS DE ESTRATÉGIAS	5
GERENCIAMENTO DE RISCOS	9
Planejamento do gerenciamento de riscos: Entradas	10
Planejamento do gerenciamento de riscos: Ferramentas e técnicas.....	11
Planejamento do gerenciamento de riscos: Saídas.....	11
REFERÊNCIAS	16



INTRODUÇÃO

O gerenciamento de riscos inclui os processos que tratam da realização de identificação, análise, respostas, monitoramento e controle e planejamento do gerenciamento de riscos. Os objetivos da gestão de riscos são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos na organização.

CONCEITOS BÁSICOS

Análise e Gestão de Riscos consiste em uma série de passos que ajudam uma equipe a entender e administrar a incerteza. Na verdade, convivemos com a incerteza o tempo todo, em maior ou menor grau, mas não nos damos conta/temos consciência dos riscos. Isto está intimamente relacionado com o conhecimento que possuímos sobre um determinado assunto. Este conhecimento pode ser tanto tácito, quanto explícito.

Alguns exemplos de riscos são atravessar uma rua, viajar (avião, automóvel ou ônibus), escolher um candidato a ocupar um cargo público, enfrentar os problemas relacionados à segurança da informação. Em outras palavras, o risco é um evento ou condição incerta que, se ocorrer, terá um efeito positivo ou negativo sobre a organização em termos de tempo, custo, qualidade, entre outros fatores. Um risco pode ter uma ou mais causas e, se ele ocorrer, um ou mais impactos:

Causa: Falta de Licença ambiental;

Impacto: Atraso no projeto devido a falta de concessão ambiental;

Causa: Falta de mão-de-obra qualificada;

Impacto: Erros/falhas na execução das atividades e tarefas devido a falta de



conhecimento sobre elas;

Causa: Vírus Eletrônico;

Impacto: Os vírus podem variar de brincadeiras de mau gosto até atingir a integridade do sistema;

Causa: Falta de Backup;

Impacto: No caso de eventuais perdas de dados, estes não podem ser recuperados.

Entretanto, a gestão de riscos normalmente aborda um risco como um problema em potencial, isto significa que o problema pode ou não acontecer. Independentemente de qual seja o resultado (positivo ou negativo), faz-se importante:

- I. Identificar o(s) risco(s);
- II. Avaliar a probabilidade de ocorrência;
- III. Estimar o seu impacto; e
- IV. Estabelecer um plano de contingência.

Na análise de risco estão todos os indivíduos envolvidos no processo, incluindo gestores, engenheiros, usuários e clientes. Todos participam, em maior ou menor grau, da análise e gestão dos riscos e todos buscam minimizar o impacto dos riscos na organização. Assim sendo, para minimizar os riscos deve-se adotar o lema do escoteiro “Estar Sempre Alerta”. Alguns empreendimentos são de difícil execução devido a alta complexidade que os envolve, o alto grau de inovação, falta de conhecimento acerca da natureza/ecossistema que permeia o empreendimento, pressão da alta gerência, altos valores envolvidos, reputação das pessoas envolvidas, entre outros.



Nas atividades das organizações, muitas coisas podem dar errado (e com frequência dão). Por este motivo é importante entender os riscos, tomar medidas preventivas e evitá-los ou administrá-los. Os principais passos envolvem o planejamento da gestão de riscos – abordar como planejar e executar as atividades de gestão de riscos, identificação de riscos – reconhecer o que pode dar errado, analisar cada risco para determinar a possibilidade da sua ocorrência e o dano causado, caso ele ocorra e um plano para administrar os riscos.

O produto do trabalho de gestão de riscos é um plano de atenuação, monitoração e gestão de riscos (Risk Mitigation, Monitoring and Management – RMMM) e um conjunto de formulários de risco.

Para garantir que a análise foi feita corretamente, os riscos devem ser analisados e geridos de acordo com um estudo que envolve as pessoas, os produtos e os projetos da organização. O plano de riscos deve ser revisto a medida que um projeto ou a própria organização evolui (atualizar os riscos) e os planos de contingência devem ser realistas. A Figura 1 ilustra a visão macro destas atividades.

Figura 1 - Visão macro





Riscos

Robert Charette (1989) no seu livro *Análise e Gestão de Riscos* apresenta que um risco afeta acontecimentos futuros. Presente e passado não preocupam “o que conhecemos hoje já foi semeado por nossas ações anteriores”. Assim, acredita-se que podemos criar oportunidade para uma situação diferente e possivelmente melhor para nós (organização) amanhã.

Risco envolve escolha e a incerteza que é inerente às escolhas dos seres humanos. Segundo Roger S. Pressman (2002), “Paradoxalmente, o Risco, como a morte e os impostos, é uma das poucas certezas da vida.”

Na economia, análise de risco é a verificação dos pontos críticos que possam vir a apresentar não conformidade durante a execução de um determinado objetivo. O termo não conformidade está intimamente ligado as causas e aos impactos de certas atividades. Exemplo: Aspectos relacionados com a alta da inflação (taxas de juros do BC); uma greve dos controladores de vôo; operações-padrão da Polícia Federal nos aeroportos; um problema com um dos parceiros da cadeia de suprimentos mundial; DoS: Denial of Service (tornar os recursos de um sistema indisponíveis para seus utilizadores), invasões e espionagem, entre outros.

O simples fato de existir uma atividade, que pode ser de qualquer natureza – conforme já apresentado, abre a possibilidade da ocorrência de eventos ou situações cujas consequências constituem oportunidades para obter vantagens (lado positivo) ou então ameaças ao sucesso (lado negativo).

TIPOS DE ESTRATÉGIAS

As estratégias são classificadas em **Reativas e Preventivas**.

Estratégias reativas a riscos são normalmente conhecidas como “Escola de Gestão



de Riscos Indiana Jones” (Pressman, 2002). Por exemplo:

- As informações foram perdidas devido uma falha de hardware, o que fazer agora?
- Descobre-se que um antigo funcionário ainda tem acesso as nossas bases de dados, quais providências devem ser tomadas?
- Um gestor-chave abandonou a empresa para trabalhar na concorrência, e agora?

Infelizmente, os gerentes não são Indiana Jones e os membros da equipe não são seus seguidores. Porém, não é pouco comum encontrar equipes que contam apenas com estratégias reativas a risco. Quando existe alguma estratégia, ela dá atenção a apenas dois aspectos:

- i) Monitoramento para riscos prováveis;
- ii) Reserva de recursos para quando eles se tornarem problemas reais.

Em geral, as equipes, que podem ser orientadas a projetos ou não, não fazem nada a respeito até que algo dê errado. Então, a equipe corre para a ação, na tentativa de corrigir o problema rapidamente, isto é comumente chamado de “Modo de combate ao fogo”.

Outra abordagem (muito mais inteligente) é ser preventivo. Mas porque as empresas muitas vezes não adotam esta vantagem? Simplesmente por pura falta de conhecimento, por que dá trabalho, e exige dedicação.

Uma boa estratégia começa antes do início dos trabalhos técnicos. O objetivo principal é evitar que os riscos negativos venham a se concretizar. Podemos então afirmar que uma estratégia de prevenção ao risco não busca apenas diminuir a probabilidade e o impacto de eventos adversos e/ou indesejáveis, mas também aumentar a probabilidade e o impacto de eventos positivos na organização.



É importante lembrar que alguns riscos são oportunidades e podem ser enfrentados em benefício da organização, como por exemplo a aceleração das atividades e tarefas e a redução de custos. Porém, nem todos os riscos podem ser evitados. Trabalha-se para o desenvolvimento de um plano de contingência e responder de modo controlado e efetivo (Figura 2).

Uma Estratégia de Prevenção inclui:

- **Planejamento do gerenciamento de riscos** – decidir como abordar, planejar e executar as atividades de gerenciamento de riscos;
- Identificação de riscos – determinar os riscos que podem afetar a organização e documentar suas características;
- **Análise qualitativa de riscos** – priorizar os riscos para análise ou ação adicional subsequente através de avaliação e combinação de sua probabilidade de ocorrência e o seu impacto;
- **Análise quantitativa de riscos** – análise numérica do efeito dos riscos identificados nos objetivos gerais da organização;
- **Planejamento de respostas a riscos** – desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos da organização;
- **Monitoramento e controle de riscos** – acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação dos novos riscos, execução de planos de respostas a riscos e avaliação da sua eficácia durante toda a vida da organização.

Esses processos interagem entre si e também com processos de outras áreas de conhecimento. Cada processo pode envolver o esforço de uma ou mais pessoas ou grupos de pessoas, com base nas necessidades da organização. Cada processo ocorre pelo menos uma vez. Embora os processos estejam



apresentados aqui como elementos distintos com interfaces bem definidas, na prática eles podem se sobrepor e interagir de maneiras não detalhadas.

O risco se origina da incerteza que está presente em todas as organizações. Os riscos conhecidos são aqueles que foram identificados e analisados, e esses riscos podem ser considerados no planejamento de ações da organização. Os riscos desconhecidos não podem ser gerenciados de forma proativa e uma resposta prudente da equipe seria alocar contingência geral contra esses riscos, e também contra todos os riscos conhecidos para os quais pode não ser econômico ou possível desenvolver uma resposta proativa.

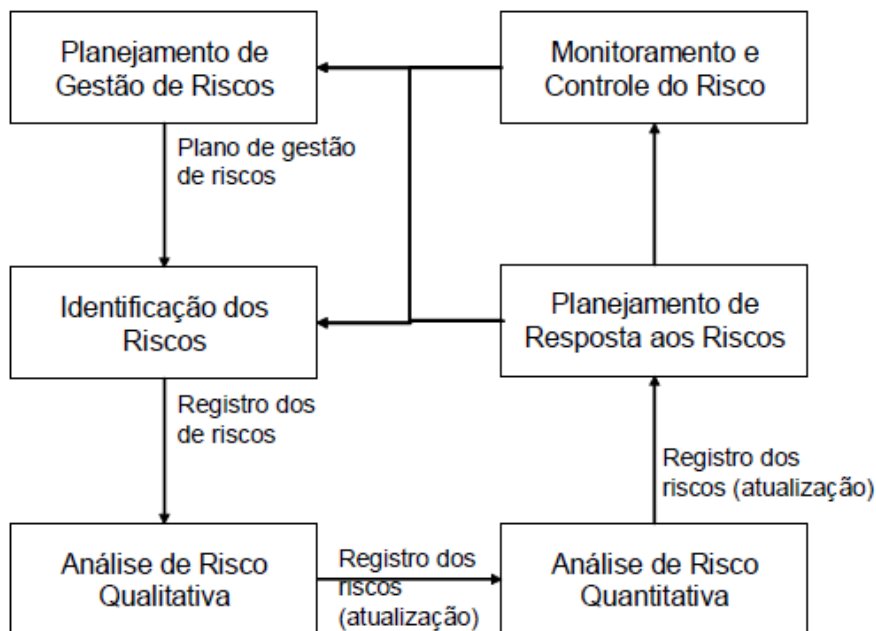
As organizações percebem os riscos quando eles estão relacionados às ameaças ao sucesso das atividades ou às oportunidades para aumentar as chances de sucesso da organização. É possível aceitar os riscos que constituem ameaças se eles forem equivalentes à premiação que pode ser obtida ao se assumir esses riscos. Os riscos que constituem oportunidades, como a aceleração do trabalho que pode ser obtida através da designação de pessoal adicional, podem ser enfrentados em benefício dos objetivos da organização.

As pessoas e, por extensão, as organizações tomam atitudes em relação aos riscos que afetam a exatidão da percepção dos riscos e a forma como respondem aos riscos. As atitudes em relação aos riscos devem ser explicitadas sempre que possível. Uma abordagem consistente do risco que atenda aos requisitos da organização deve ser desenvolvida para cada situação específica ou projetos, e a comunicação do risco e o seu tratamento devem ser abertos e transparentes. As respostas a riscos refletem o equilíbrio entre enfrentar riscos e evitar riscos considerados por uma organização.

Para ser bem-sucedida, a organização deve estar comprometida com uma abordagem de gerenciamento de riscos proativa e consistente.



Figura 2 - Fluxograma de processo do gerenciamento de riscos



GERENCIAMENTO DE RISCOS

Um planejamento cuidadoso e explícito aumenta a possibilidade de sucesso dos outros cinco passos do gerenciamento de riscos. O planejamento do gerenciamento de riscos é o processo de decidir como abordar e executar as atividades de gerenciamento de riscos. O planejamento dos processos de gerenciamento de riscos é importante para garantir que o nível, tipo e visibilidade do gerenciamento de riscos estejam de acordo com o risco e a importância de um projeto ou um processo em relação à organização, para fornecer tempo e recursos suficientes para as atividades de gerenciamento de riscos e para estabelecer uma base acordada de avaliação de riscos (Figura 3).



Figura 3 - Planejamento do gerenciamento de riscos: Entradas, ferramentas e técnicas, e saídas

Entradas	Ferramentas e Técnicas	Saídas
<ol style="list-style-type: none">1. Fatores ambientais da empresa2. Ativos de Processos organizacionais3. Declaração de escopo	<ol style="list-style-type: none">1. Análise e reuniões de planejamento	<ol style="list-style-type: none">1. Plano de gerenciamento de riscos2. Definição de probabilidade de impacto dos riscos

Planejamento do gerenciamento de riscos: Entradas

Fatores ambientais da empresa

As atitudes em relação ao risco e a tolerância a risco das organizações e pessoas envolvidas influenciarão o plano de gerenciamento. As atitudes e tolerâncias a risco podem ser expressas em declarações de políticas ou reveladas em ações.

Ativos de processos organizacionais

As organizações podem possuir abordagens predefinidas em relação ao gerenciamento de riscos, como categorias de risco, definição comum de conceitos e termos, modelos padrão, funções e responsabilidades padrão, e níveis de autoridade para a tomada de decisões.



- Declaração do escopo
- Plano de gerenciamento

Planejamento do gerenciamento de riscos: Ferramentas e técnicas

Análise e reuniões de planejamento

As equipes realizam reuniões de planejamento para desenvolver o plano de gerenciamento de riscos. Os participantes dessas reuniões podem incluir o gerente de projetos, membros da equipe do projeto selecionados e partes interessadas, qualquer pessoa da organização que tenha responsabilidade no gerenciamento das atividades de execução e planejamento de riscos, e outras pessoas, conforme necessário.

Os planos básicos para executar as atividades de gerenciamento de riscos são definidos nessas reuniões. Serão desenvolvidos os elementos de custo de riscos e as atividades do cronograma de riscos para serem incluídos no orçamento e cronograma da organização. Serão designadas as responsabilidades de riscos. Modelos organizacionais gerais para categorias de risco e definições de termos como níveis de risco, probabilidade por tipo de risco, impacto por tipo de objetivos, além da matriz de probabilidade e impacto, serão adaptados para caso específico. As saídas dessas atividades serão resumidas no plano de gerenciamento de riscos.

Planejamento do gerenciamento de riscos: Saídas

Plano de gerenciamento de riscos

O plano de gerenciamento de riscos descreve como o gerenciamento de riscos será estruturado e executado na organização. O plano de gerenciamento



de riscos inclui:

- **Metodologia.** Define as abordagens, ferramentas e fontes de dados que podem ser usadas para executar o gerenciamento de riscos.
- **Funções e responsabilidades.** Define a liderança, suporte e participação da equipe de gerenciamento de riscos em cada tipo de atividade do plano de gerenciamento de riscos, designa pessoas para essas funções e esclarece suas responsabilidades.
- **Orçamentação.** Designa recursos e estima os custos necessários para o gerenciamento de riscos.
- **Tempos.** Define quando e com que frequência o processo de gerenciamento de riscos será executado e estabelece as atividades de gerenciamento de riscos que serão incluídas no cronograma.
- **Categorias de risco.** Fornece uma estrutura que garante um processo abrangente para identificar sistematicamente os riscos até um nível consistente de detalhes e contribui para a eficácia e qualidade da identificação de riscos. Uma organização pode usar uma categorização previamente preparada dos riscos típicos. Uma estrutura analítica dos riscos (EAR) (Figura 4) é uma abordagem para fornecer essa estrutura, mas ela pode também ser realizada através da simples listagem dos diversos aspectos da organização. As categorias de risco podem ser reexaminadas durante o processo Identificação de riscos. Uma boa prática é revisar as categorias de risco durante o processo Planejamento do gerenciamento de riscos antes de usá-las no processo Identificação de riscos. As categorias de risco que se baseiam em ações/projetos anteriores podem precisar ser

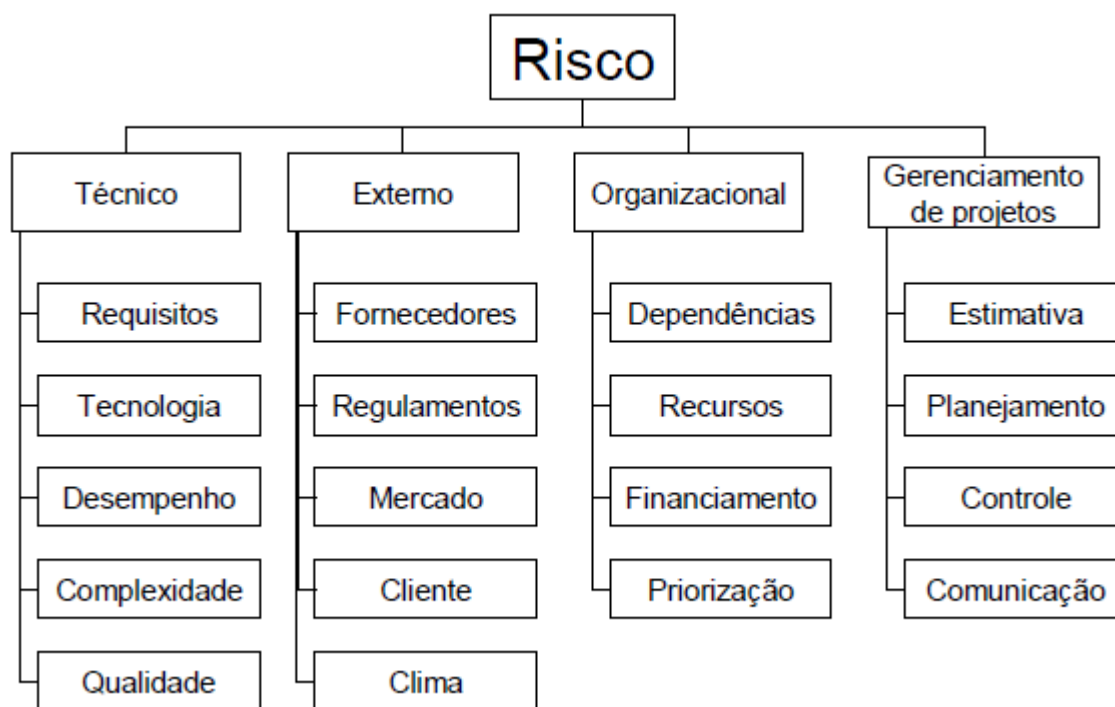


ampliadas, ajustadas ou adequadas a novas situações antes de poderem ser usadas.

- Definições de probabilidade e impacto de riscos. A qualidade e credibilidade do processo Análise qualitativa de riscos exigem a definição de níveis diferentes de probabilidades e impactos de riscos. As definições gerais dos níveis de probabilidade e impacto são adequadas ao projeto individual durante o processo Planejamento do gerenciamento de riscos para serem usadas no processo Análise qualitativa de riscos.

Poderia ser usada uma escala relativa representando os valores das probabilidades desde “muito improvável” até “quase certeza”. Alternativamente, é possível usar probabilidades numéricas atribuídas em uma escala geral (por exemplo, 0,1; 0,3; 0,5; 0,7; 0,9). Outra abordagem para calibrar a probabilidade envolve o desenvolvimento de descrições do estado das ações relacionadas ao risco que está sendo considerado.

Figura 4 - Exemplo de uma estrutura analítica dos riscos (EAR)



A escala de impacto reflete a importância do impacto, negativa para ameaças ou positiva para oportunidades. As escalas de impacto são específicas do objetivo potencialmente afetado, da situação financeira e estratégias da organização e da sensibilidade da organização a impactos específicos. As escalas relativas de impacto são descritas e classificadas de forma simples, como “muito baixo”, “baixo”, “moderado”, “alto” e “muito alto”, refletindo impactos cada vez maiores conforme definido pela organização. Alternativamente, as escalas numéricas atribuem valores a esses impactos. Esses valores podem ser lineares (por exemplo, 0,1; 0,3; 0,5; 0,7; 0,9) ou não lineares (por exemplo, 0,05; 0,1; 0,2; 0,4; 0,8). As escalas não lineares podem representar o desejo da organização de evitar ameaças de alto impacto ou de explorar oportunidades de alto impacto, mesmo se elas tiverem uma probabilidade relativamente baixa. No uso de escalas não lineares é importante entender o significado dos números e como se relacionam entre si, como são derivados e o efeito que podem ter sobre os



diversos objetivos da organização.

A Figura 5 é um exemplo de impactos negativos de definições que poderiam ser usadas na avaliação dos impactos de riscos relacionados a quatro objetivos. Essa figura ilustra tanto as abordagens relativas como as numéricas (neste caso, não linear). A figura não pretende indicar que os termos relativos e numéricos são equivalentes, mas sim mostrar as duas alternativas em uma figura em vez de em duas.

Figura 5 - Definição de escalas de impacto para quatro objetivos

Condições definidas para as escalas de impacto de um risco em objetivos importantes (impactos negativos)					
Objetivo	Muito Baixo 0,05	Baixo 0,10	Moderado 0,20	Alto 0,40	Muito alto 0,80
Custo	Aumento de custo não significativo	Aumento de custo < 10 %	Aumento de custo de 10% a 20%	Aumento de custo de 20% a 40%	Aumento de custo > 40%
Tempo	Aumento de tempo não significativo	Aumento de tempo < 5%	Aumento de tempo de 5% a 10%	Aumento de tempo de 10% a 20%	Aumento de tempo > 20%
Escopo	Diminuição do escopo quase imperceptível	Áreas menos importantes do escopo afetadas	Áreas importantes do escopo afetadas	Redução do escopo inaceitável	Item final sem nenhuma utilidade
Qualidade	Degradação da qualidade quase imperceptível	Somente aplicações mais críticas afetadas	Redução da qualidade exige aprovação do patrocinador	Redução da qualidade inaceitável	Item final sem nenhuma utilidade

- Matriz de probabilidade e impacto. Os riscos são priorizados de acordo com suas possíveis implicações para o atendimento dos objetivos. A abordagem típica de priorização de riscos é usar uma tabela de pesquisa ou uma matriz de probabilidade e impacto. As combinações específicas de probabilidade e impacto que podem fazer com que um risco seja classificado como de importância “alta”, “moderada” ou “baixa” juntamente com a importância correspondente para o planejamento de respostas ao



risco são normalmente definidas pela organização. Elas são revisadas e podem ser adequadas ao projeto específico durante o processo planejamento do gerenciamento de riscos.

Definição de escalas de impacto para quatro objetivos do projeto

- Revisão das tolerâncias das partes interessadas. As tolerâncias das partes interessadas podem ser revisadas no processo Planejamento do gerenciamento de riscos, pois se aplicam a um projeto específico.
- Formatos de relatório. Descreve o conteúdo e formato do registro de riscos, além de outros relatórios de riscos necessários. Define como serão documentados, analisados e comunicados os resultados dos processos de gerenciamento de riscos.
- Acompanhamento. Documenta como todos os aspectos das atividades de risco serão registrados em benefício da organização, das necessidades futuras e das lições aprendidas. Documenta se os processos de gerenciamento de riscos passarão por auditoria e como isso será feito.

REFERÊNCIAS

BACCARINI, David; ARCHER, Richard, 2001. **The risk ranking of projects: a methodology.** International Journal of Project Management 19 (2001) 139-145.

BARBER, Richard B. 2005; **Understanding internally generated risks in projects.** In: International Journal of Project Management 23 (2005) 584-590.

BRODER, James F.; **Risk Analysis and the Security Survey.** Boston: Butterworth - Heinemann, 2ª edição, 2000.



BRASILIANO, Antônio Celso Ribeiro. **Planejamento de Segurança Empresarial- Metodologia e Implantação**. S.Paulo, Cia. Das Artes, 1999.

BRASILIANO, Antônio Celso Ribeiro. **Risk Net: Aumentando a Eficácia no Monitoramento**. Revista Proteger, S.Paulo, número 41, pg. 40 à 48, 2002.

CHAPMAN, Robert J.; **The controlling influences on effective risk identification and assessment for construction design management**. In: International Journal of Project Management 19 (2001) 147-160. 2001.

CHARETTE, R. N.; 1992; **Building Bridges over Intelligent Rivers**". In: American Programmer, vol 5, nro 7 Semptember 1992, 2-9.

WARD, Stephen; CHAPMAN, Chris; **Transforming project risk management into project uncertainty management**. In: International Journal of Project Management 21 (2003) 97-105.

COPPER, Dale F.; GREY, Stephen; RAYMOND, Geoffrey; WALKER, Phil; **Project risk management guidelines: managing risk in large projects and complex procurements**, John Wiley & Sons Ltda. 2005.

GORDON, Lawrence A.; LOEB, Martin P.; LUCYSHYN, William; RICHARDSON, Robert. 2006. **CSI/FBI Computer Crime and Security Survey**. Disponível em <http://www.gocsi.com>. Acesso em 05 de Janeiro de 2007.



GARP, FRM. Exam Review Class Notes. **Risk Analysis Techniques**. 1998.

HARDY, M.: **Modeling and Risk Management for Equity-Linked Life Insurance**. John Wiley & Sons, Inc. 2003.

KEIL, Mark; CULE, Paul E.; LYYTINEN, Kall; SCHMIDT, Roy C.; **A Framework for Identifying Software Project Risks**. In: COMMUNICATIONS OF THE ACM November 1998/Vol. 41, No. 11.

PMBOK, **Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos** - Terceira edição. Project Management Institute, Inc. Four Campus Boulevard, 2004.

PRESSMAN, Roger S. **Engenharia de Software** – Quinta edição. McGraw-Hill, 2002.

Stoneburner, Gary; Goguen, Alice ; Feringa, Alexis. **Risk Management Guide for Information Technology Systems**. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30
Manual of Corporate and Industrial Security. Englewood: Prentice Hall, 1992.