A aplicação de modelos de decisão como auxílio à análise de risco no contexto da Auditoria de Sistemas

Cristiane Yayoko Ikenaga
Centro Estadual de Educação Tecnológica Paula Souza
crisikenaga@uol.com.br

Napoleão Verardi Galegale
Centro Estadual de Educação Tecnológica Paula Souza
nvg@galegale.com.br

Resumo

A análise de risco é um processo que envolve fatores objetivos e crenças subjetivas de avaliação e, muitas vezes, é utilizada para subsidiar decisões estratégicas nas organizações. No contexto da Auditoria de Sistemas, estas decisões estratégicas estão relacionadas à promoção de melhor utilização de recursos disponíveis, quais sejam, computacionais, humanos, financeiros e operacionais. Também estão relacionadas à implementação de controles ou mecanismos que minimizem a ocorrência de problemas e/ou impactos relacionados a esses recursos.

A diversidade de modelos para a tomada de decisão é objeto deste estudo, na medida em que eles podem vir a auxiliar o processo de avaliação de risco no contexto da Auditoria de Sistemas. Tais modelos, de análise teórica do campo da Teoria da Administração e das Organizações, são apresentados com o objetivo de analisá-los à luz da aplicação em processos de análise de risco, considerados processos de tomada de decisão.

Por modelos de decisão, deve-se entender, no contexto deste artigo, o processo de modelagem de um problema e a solução do modelo como apoio à tomada de decisão.

O objetivo principal deste estudo é identificar as características de alguns modelos de decisão e sua aplicação no processo de avaliação de risco, além de apresentar diferentes modelos de decisão e detalhar a estrutura do processo decisório e os elementos nele envolvidos a partir de um estudo exploratório baseado em uma revisão bibliográfica.

Este trabalho não tem a pretensão de exaurir o assunto tampouco aprofundar em detalhes cada tipo de modelo de decisão, mas sim, levantar algumas características relevantes de algumas abordagens de decisão e visualizar a análise de risco nos trabalhos de auditoria de sistemas como um processo decisório que pode se basear em modelos de decisão.

Palavras-chave: Modelos de decisão, Processos de decisão, Análise de risco, Auditoria de sistemas

Introdução

As organizações estão cada vez mais dependentes de seus sistemas de informação e das tecnologias de informação. Esses recursos já não são considerados como simples apoio à execução das atividades, mas sim, são recursos estratégicos e críticos de manutenção de suas operações. Além disso, são também considerados ativos (*assets*) da organização.

Um dos objetivos da Auditoria de Sistemas é avaliar os sistemas de informação e o ambiente em que estes estão inseridos, adequando-os segundo alguns parâmetros tais como

eficiência, eficácia entre outros. Decorrem da avaliação os processos de revisão e de acompanhamento. Outro objetivo é promover a adequação na utilização de recursos humanos, materiais e tecnológicos envolvidos no ambiente de sistemas de informação.

Os propósitos dos trabalhos de auditoria de sistemas possibilitam que a organização gerencie seus sistemas de informação, tecnologias de informação e o seu ambiente computacional, de maneira a minimizar problemas decorrentes de falhas, erros, ineficiência etc. nestes recursos ou, em outras palavras, para minimizar riscos por meio da implementação de controles de segurança e estabelecimento de requisitos de segurança, tendo sempre em vista o alinhamento com os objetivos, com a visão e a missão da organização.

Controles de segurança são mecanismos ou parâmetros que podem ser implementados nos sistemas de informação ou no ambiente em que estes estão inseridos com o objetivo de minimizar falhas ou erros e garantir que os objetivos específicos de segurança desses recursos (por exemplo: confidencialidade e integridade das informações) sejam atendidos.

A avaliação de risco possibilita identificar ameaças e vulnerabilidades relacionadas aos sistemas de informação, tecnologias de informação e demais ativos e, uma vez identificadas, possibilita avaliar a probabilidade dessas ameaças ocasionarem um problema, e estimar o impacto potencial caso essas ameaças se concretizem.

O nível de risco de cada item avaliado pode ser obtido a partir de cálculos de probabilidades de ocorrência, contudo, mesmo que se obtenha uma representação quantitativa, a percepção de risco é, por sua vez, um processo complexo e subjetivo, pois, além de depender de um ponto de referência pessoal, pode ser alterada conforme o contexto e no decorrer do tempo.

Ao não utilizar uma metodologia adequada para avaliação de risco, a eficácia do processo pode ficar comprometida, na medida em que a organização não estabelece os propósitos, os critérios, o nível de risco aceitável e outros parâmetros inerentes à avaliação.

A avaliação do risco, ou melhor, a percepção do risco e seu julgamento fazem parte de um processo de tomada de decisão. Processo este que envolve sentimentos, valores e interpretações pessoais, ao mesmo tempo em que não deixa a racionalidade de lado. Porque não se trata de elementos excludentes, mas sim, complementares.

Metodologia

A metodologia de pesquisa é um estudo exploratório baseado em uma revisão bibliográfica, a fim de organizar os conceitos e modelos de decisão, seguida de uma análise crítica de sua aplicabilidade, tendo como foco o processo de avaliação de risco na Auditoria de Sistemas.

De acordo com Selltiz et al. [13], os estudos exploratórios “têm o propósito de formular um problema para investigação mais exata, ou desenvolver hipóteses” e classifica-os em levantamento da literatura, levantamento de experiências e análise de exemplos. Ainda para Selltiz et al., o acúmulo de atividades e decisões na rotina de um projeto ou atividade social adquire um “reservatório de experiência que podem ser de valor incalculável”.

Para Gil [9], “as pesquisas exploratórias têm como principal finalidade desenvolver, esclarecer e modificar conceitos e idéias, com vistas na formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores”.

Cooper e Schindler [7] consideram que “através da exploração, os pesquisadores desenvolvem conceitos de forma mais clara, estabelecem prioridades, desenvolvem definições operacionais e melhoram o planejamento final da pesquisa. (...) A exploração também serve a outros objetivos. A área de investigação pode ser tão nova ou tão vaga que o pesquisador precisa fazer uma exploração a fim de saber algo sobre o problema.”

Resultados

Objetivos e atividades de Auditoria de Sistemas

Attie [3] afirma que o objetivo principal da auditoria pode ser descrito como sendo "o processo pelo qual o auditor se certifica da veracidade das demonstrações financeiras preparadas pela companhia auditada.". Complementa ainda considerando que o auditor, em seu exame, "por um lado, utiliza os critérios e procedimentos que lhe traduzem provas que assegurem a efetividade dos valores apostos nas demonstrações financeiras e, por outro lado, cerca-se dos procedimentos que lhe permitem assegurar a inexistência de valores ou fatos não constantes das demonstrações financeiras que sejam necessários para seu bom entendimento."

A auditoria é uma atividade que compreende a avaliação de operações, processos, sistemas e responsabilidades gerenciais de uma entidade e seu propósito é, entre outros, verificar a conformidade da execução dessas operações, processos etc. em relação a regras, normas, políticas, leis e outros instrumentos, com o propósito de satisfazer, no que lhe diz respeito, o atendimento dos objetivos de negócio da organização.

A atividade de auditoria de sistemas, por sua vez, está relacionada à avaliação de sistemas de informação, do ambiente computacional, da segurança das informações e também dos controles internos da organização.

Controles e Controles Internos

Os controles são instrumentos que visam minimizar problemas de segurança dos sistemas de informação, do ambiente computacional e dos recursos humanos envolvidos direta ou indiretamente e podem estar integrados ou não aos recursos computacionais. Eles podem ser:

- Preventivos: para evitar erros, falhas bem como promover a aplicação de boas práticas de uso e gerenciamento desses recursos e do ambiente;
- Detectivos: para identificar o problema. Nos casos em que o fator de causa é também identificado, ações devem ser direcionadas para que seja implementada a correção do problema em questão (quando se verificar possível) bem como controles preventivos para evitar a ocorrência do mesmo incidente ou de problemas similares;
- Corretivos: para sanar o problema ocorrido e para que o impacto seja o menor possível.

Cabe ressaltar que a implementação de controles não elimina todos os problemas possíveis de uma organização e seu ambiente computacional, mas vem a aumentar a confiabilidade nos processos e operações.

Verificar se a organização tem como prática adotar e implementar controles ou controles internos, como são denominados, é uma das atividades da Auditoria de Sistemas, e assegurar a adequação de controles implantados e utilizados é um de seus objetivos.

Segundo o American Institute of Certified Public Accounts (AICPA), controle interno é "o plano de organização e todos os métodos e medidas coordenados, aplicados em uma empresa, a fim de proteger seus bens, conferir a exatidão e a fidelidade de seus dados contábeis, promover a eficiência e estimular a obediência às diretrizes administrativas estabelecidas", conforme definição apresentada em 1949, em seu Relatório Especial da Comissão de Procedimentos de Auditoria.

Arima [1] apresenta a classificação dos controles internos em dois subconjuntos:

- Controles internos contábeis
  - Fidelidade da informação em relação ao dado;

  - Segurança física;
  - Segurança lógica;
  - Confidencialidade (*privacy*);
  - Obediência à legislação em vigor
- Controles internos administrativos
  - Eficácia;
  - Eficiência;
  - Obediência às diretrizes da alta administração

Os controles internos contábeis dizem respeito à proteção dos bens da organização e à verificação da exatidão e da veracidade das informações contábeis. Os controles internos administrativos, por sua vez, estão relacionados aos processos estratégicos de decisão da organização.

Evidentemente, a implementação de controles deve ser observada com cuidado e a organização deve levar em consideração, principalmente, suas reais necessidades, haja vista que controles em excesso, desnecessários, inadequados ou mal aplicados podem dificultar a utilização dos recursos de informação (sistemas, tecnologias de informação etc.), causando um impacto nas operações que mantêm a organização. Outro item a ser considerado são os custos relacionados à implementação de controles. Por outro lado, a ausência de controles acarreta em questões como exposição às vulnerabilidades inerentes do ambiente computacional, não disponibilidade de recursos de informação etc.

O ideal, portanto, é equilibrar a adoção de controles para o bom funcionamento e utilização dos recursos da organização, sejam eles tecnológicos, materiais, financeiros ou humanos, visando a operação, continuidade de serviços e, sem dúvida, o sucesso da organização.

Encontrar o ponto ótimo que traduza a melhor combinação de controles e custos em função da obtenção de segurança, de eficiência e de eficácia, ou seja, sem comprometer a integridade, a confiabilidade e a confidencialidade das informações e a disponibilidade de acesso aos recursos de informação, é parte de um processo em que a organização deve estabelecer uma faixa aceitável dessa combinação. Significa reconhecer que a implementação de controles visa minimizar os riscos e aumentar o grau de segurança a uma faixa ou a um nível aceitável, de maneira que não sejam colocados em risco os objetivos de negócio da organização.

Ocorre, muitas vezes, das organizações sequer saberem quais os ativos que devem ser efetivamente protegidos e que tipo de proteção é realmente necessário.

A análise e a avaliação de risco são, neste sentido, um instrumento que possibilita auxiliar o processo de auditoria de sistemas indicando, quais ativos devem ser priorizados quanto à implementação de controles e medidas de proteção.

Objetivos e atividades de Análise de Risco

A análise de risco é um processo que abrange controles e procedimentos operacionais, físicos, técnicos, pessoais e até mesmo administrativos com o propósito de:

- Identificar os ativos de negócio;
- Identificar, reconhecer e mensurar as ameaças relacionadas a esses ativos;
- Analisar as vulnerabilidades;
- Avaliar o nível do impacto no negócio, caso as ameaças se concretizem;
- Proporcionar a adoção de medidas apropriadas para proteger recursos e ambiente computacional da organização, bem como os recursos humanos envolvidos.

A NBR ISO/IEC 17799:2005 [2], no contexto da segurança da informação, apresenta a análise e avaliação de risco como uma consideração sistemática de “estimar a magnitude do

risco (análise de riscos) e o processo de comparar os riscos contra os critérios de risco para determinar a significância do risco (avaliação do risco)".

Broder [5] define ativo como "o que uma empresa tem, opera, controla, usa, tem a custódia sobre, tem a responsabilidade sobre, compra, vende, produz, projeta, manufatura, testa, analisa ou mantém".

Por sua vez, pode-se entender por ameaça um processo que, quando ativado, pode destruir ou danificar ativos.

Vulnerabilidades podem ser entendidas como uma característica ou propriedade de um ativo ou grupo de ativos que pode ser explorada por uma ameaça, ocasionando perdas ou danos. Em outras palavras, trata-se de fraquezas nos controles e que podem ser exploradas, catalisando a concretização da ameaça.

Pode-se entender por impacto ou impacto no negócio, a conseqüência de um incidente esperado ou não, acidental ou deliberado, que venha a afetar um ou mais ativos da organização, causando, neste sentido, problemas relacionados à perda de disponibilidade, de integridade, de confidencialidade, de autenticidade, perdas financeiras e, até mesmo, a destruição de um ativo.

Ciechanowicz [6] sintetiza a definição de análise de risco como sendo "um processo para identificar riscos de segurança, determinar sua magnitude e identificar as áreas e os ativos que necessitam de controles".

Risco ou grau de risco deve ser entendido como o potencial que uma dada ameaça explora em relação à vulnerabilidade de um ativo ou grupo de ativos, podendo vir a causar perdas ou danos a esse(s) ativo(s). Em outras palavras, trata-se da probabilidade de uma ameaça acontecer, causando um problema.

A principal finalidade de uma análise de risco é auxiliar o processo de tomada de decisão da organização em relação a estabelecer quais tipos de controle são realmente necessários. A quantidade e o nível de proteção a ser implementado em um sistema de informação, nos recursos de tecnologia da informação e comunicação de uma organização são decisões estratégicas de negócio. Não existe uma relação de controles e contramedidas que se aplicam a qualquer tipo de organização. Cada entidade deve avaliar quais os controles mais adequados à sua realidade e necessidades, além de avaliar o nível aceitável de riscos em relação a cada tipo de ameaça identificada ou, em análises mais detalhadas, o nível de risco residual que a organização está preparada a aceitar.

Risco residual, portanto, deve ser entendido como o risco que permanece mesmo após a implementação de controles. Cabe ressaltar que o nível de risco residual que a organização está preparada a aceitar não significa, em momento algum, o risco que a organização pode ignorar, pelo contrário, trata-se de riscos assumidos e, portanto, conhecidos.

A avaliação de risco pode ser mensurada em termos de medida quantitativa (probabilidade, por exemplo) ou de medida qualitativa (tal como uma escala: alta, média e baixa).

A análise de risco quantitativa é uma abordagem matemática na qual as alternativas de soluções têm como base o cálculo da probabilidade de ocorrência de determinados eventos. A análise qualitativa, por sua vez, denota uma perspectiva mais subjetiva, com classificações de escala do tipo alto/médio/baixo. Em outras palavras, pode-se dizer também que a análise qualitativa é utilizada quando a organização não dispõe de registros confiáveis sobre a materialização de seus riscos.

Os elementos do processo de análise de risco

A análise de risco, seja ela efetuada por meio de um processo qualitativo ou quantitativo, compreende, em geral, os seguintes elementos: ativo(s) ou grupo de ativos, ameaça(s), vulnerabilidade(s), impacto(s), escala de impactos, escala de vulnerabilidades,

categorias de risco e prioridades de ação, possibilidades e probabilidade de ocorrência, e fatores de risco associados. O Quadro 1 apresenta uma sugestão de escala de impactos.

Quadro 1 – Escala de classificação de impactos

Impacto	Descrição
1 – Imaterial	Efeito pouco significativo, sem afetar a maioria dos processos de negócios da organização; perdas financeiras irrelevantes.
2 – Baixo	Sistemas de informação e/ou operações não disponíveis por um período de tempo dentro da faixa definida como aceitável; perda de credibilidade junto aos clientes e mercado em geral; pequenas perdas financeiras
3 – Médio	Sistemas de informação e/ou operações críticas não disponíveis por um período de tempo acima do definido como aceitável; perdas financeiras de vulto considerável.
4 – Alto	Efeitos desastrosos, porém sem comprometer a sobrevivência da organização; perdas financeiras de vulto significativo.
5 – Crítico	Efeitos desastrosos, comprometendo a sobrevivência da organização.

Fonte: Adaptado de Dias [8]

No processo de avaliação de risco, além de identificar as vulnerabilidades relacionadas a uma determinada ameaça, é também interessante classificá-las conforme algum critério predeterminado, para uma análise mais detalhada. O Quadro 2 apresenta uma sugestão de escala de vulnerabilidades.

Quadro 2 – Escala de classificação de vulnerabilidades

Vulnerabilidade	Descrição
Alta	Existência de fraquezas significativas nos sistemas ou nos processos operacionais com impacto significativo. Controles devem ser, necessariamente, implementados.
Média	Existência de algumas fraquezas com impacto significativo. Controles devem ser implementados.
Baixa	Não foram identificadas fraquezas e os sistemas estão operando corretamente. Controles adicionais não são necessários.

Fonte: Nosworth [12]

Para direcionar ações conforme cada situação analisada, convém priorizá-las. Neste sentido, é possível orientar-se a partir do grau de risco identificado ou conforme uma classificação de risco, como a apresentada a seguir, no Quadro 3.

Quadro 3 – Categorização de risco

Categoria	Prioridade de ação
A	É necessária a implementação imediata de ações corretivas, bem como a redução de vulnerabilidades ou a redução do nível de impacto, ou ambos. O controle desses riscos é de prioridade alta.
B	É necessário planejar ações corretivas apropriadas e executá-las para reduzir a vulnerabilidade ou o nível de impacto, ou ambos.
C	Os riscos, neste caso, são considerados aceitáveis porque ou a vulnerabilidade é baixa (menor grau) ou o impacto é menor, mas eles devem ser monitorados para garantir que eles não virão a ser classificados como riscos da categoria “B”.
D	Nenhuma ação é necessária.

Fonte: Nosworth [12]

Todos esses elementos que compreendem o processo de análise de risco devem ser avaliados e interpretados de acordo com as necessidades e a realidade do processo, da área ou da organização que estiver sendo avaliada. Assim, deve-se também levar em consideração o nível de granularidade de uma análise de riscos. Desta maneira, é possível não perder o foco

de atenção em relação a uma questão, ao mesmo tempo que pode-se detalhar o quanto for necessário um problema envolvendo um grau de risco identificado como alto.

Modelos de decisão e a análise de risco como processo de tomada de decisão

A análise de risco pode ser entendida como um processo de resolução de problemas e de formulação de alternativas de decisão e, neste sentido, um processo de tomada de decisão. Diversos são os modelos de decisão utilizados pelas organizações e estudados por pesquisadores. Toda decisão implica uma ação, mesmo que seja a ação de nada fazer ou nada mudar. Neste sentido, a não decisão é também uma decisão.

Uma decisão é difícil de ser tomada porque pode ser complexa, estar inserida em um contexto de indecisão, riscos, ou ainda, de conflitos. Conhecer modelos, processos e estruturas de decisão não garantirá soluções efetivas, mas possibilitará conhecer táticas e estratégias para melhorar a probabilidade de sucesso de uma decisão, afinal, ações bem sucedidas requerem muito mais que apenas boas intenções, baseadas em crenças pessoais. E boas intenções, por sua vez, não são garantia de boas decisões.

Teorias e modelos de decisão organizacionais são probabilísticos e não determinísticos. Explica-se: seriam determinísticos se todas as hipóteses e cenários compreendessem variáveis de magnitude conhecida, mas “entre as variáveis que ocorrem no modelo, algumas são controláveis, isto é, restringidas pelo desejo de quem toma a decisão dentro de um campo específico de valores. Outras não são assim.” [11].

Modelos são representações simplificadas da realidade, isto é, do mundo real. Os modelos de decisão podem não ser completos mas conhecê-los certamente auxilia no processo de desenvolvimento de estratégias e direcionamento de ações.

O **modelo clássico da teoria de decisão**, também denominado estratégia de otimização, é aquele em que o tomador de decisão deve buscar e escolher a melhor alternativa que maximize a consecução dos objetivos da organização [10]. Este modelo sugere a seqüência de um plano de ação racional e bem estruturado. Ocorre que, muitas vezes, não se tem todas as informações necessárias, ou ainda, não se tem acesso a todas as informações relevantes ao processo de tomada de decisão. Entretanto, pode ocorrer que [4]:

> A informação de que você dispõe não é a informação que você deseja.
> A informação que você deseja não é a informação que você necessita.
> A informação que você necessita não é a informação que você consegue obter.
> A informação que você consegue obter custa mais do que você deseja pagar.

Kaufmann [11] observa que “os problemas que envolvem o homem são essencialmente de natureza combinatória [...] com alternativas que podem combinar-se n a n”. Nem sempre é possível antecipar ou prever todas as alternativas de solução bem como todas as conseqüências possíveis. Esta situação se deve, em parte, ao fato da incerteza de eventos futuros. Além disso, sob condições de incerteza, não há resposta única.

Hoy e Tarter [10] argumentam que a racionalidade é limitada não somente pela incerteza das situações e restrição de conhecimento dos tomadores de decisão mas também porque essas pessoas podem se valer de tendências inconsistentes e de propósitos que podem levar ao desvio dos objetivos traçados inicialmente pela organização. Os autores afirmam ainda que os indivíduos são incapazes de tomar decisões completamente racionais em contextos complexos e, portanto, podem acabar por buscar soluções satisfatórias no contexto de sua realidade.

No contexto da tomada de decisão, os problemas podem ser classificados em (TURBAN e ARONSON (1998) apud SHIMIZU [14]):

- Estruturados ou bem definidos: aqueles cuja definição e fases de operação para chegar aos resultados desejados estão bem claras e sua execução repetida é sempre possível;

- Semi-estruturados: são aqueles com operações bem conhecidas, mas que contêm algum fator ou critério variável que pode influenciar no resultado;
- Não estruturados: neste caso, tanto os cenários como o critério de decisão não estão fixados ou conhecidos a priori.

Os **modelos de decisão racionais** são assim caracterizados basicamente por basear-se em regras, rotinas e planos de ação bem estruturadas. São modelos que buscam pela solução a partir da aplicação de algumas regras de raciocínio, de forma correta ou, até mesmo, incorreta. Esse tipo de modelo não significa, necessariamente, um modelo de decisão infalível. Tais modelos lidam com decisão sem risco, decisão com solução ótima e decisão com solução satisfatória, e decisão com uso de técnicas heurísticas.

Os **modelos processuais**, por sua vez, têm como características apresentar problemas com um nível de incerteza e de imprecisão maior que os modelos racionais, em cenários e objetivos únicos ou múltiplos. Esses modelos lidam com decisão em situação de incerteza ou risco.

Modelos ambíguos têm como características apresentar problemas com um nível de incerteza e de imprecisão alto e em contextos com conflitos de objetivos e ambigüidade. Um exemplo é o modelo de decisão da lata do lixo, conhecido também como *garbage can model*, é uma analogia do problema de tomada de decisão a uma lata de lixo, na qual os problemas a serem resolvidos são nela depositados ou jogados.

Já os **modelos políticos** têm como características apresentar problemas com conflitos de objetivos (geralmente objetivos múltiplos), conflitos de interesse e de negociação. Esses modelos geralmente levam em consideração aspectos como o poder, a influência e a autoridade e lidam com decisão com incerteza, múltiplos objetivos e múltiplos cenários.

Modelos de decisão podem vir a auxiliar um processo de análise de risco na organização, uma vez que o estudo sobre eles permite conhecer e ter contato com exemplos de formulação e resolução de problemas, além de possibilitar aguçar e desenvolver novas estratégias de soluções. A idéia principal aqui está em “aprender”, inclusive pela praxiologia, isto é, pelo estudo (ciência) da ação.

Decisões e ações bem sucedidas necessitam muito mais que apenas boas intenções. E boas intenções, por sua vez, não são garantia de boas decisões. As pessoas têm diferentes níveis de incerteza quando apresentadas ao mesmo problema a ser resolvido. Da mesma maneira, apresentam diferentes formas de reagir ao mesmo problema. “Um negócio não pode ser conduzido apenas com sutileza ou mesmo astúcia. Tem-se que ver os fatos e as situações traçadas tão exatamente quanto possível. Modelos devem ser produzidos nos quais as discussões possam ser baseadas, modelos cada vez mais perto da realidade; talvez incompletos, porque eles são modelos e não objetos, mas solidamente construídos em bases lógicas” [11].

Há que se atentar, porém, para as armadilhas que podem fazer parte no processo de decisão, no que se refere à formulação e estruturação de um problema.
É desejável, para não dizer necessário, que a escolha possa ser justificada de maneira clara, e não, ambígua.

Hammond, Keeney e Raiffa apud Shimizu [14], relacionam algumas situações que podem levar a uma má decisão. São elas:

- Armadilha da âncora: fixação no histórico, na tendência mundial ou na tradição;
- Armadilha do status quo: acomodamento para não sair da situação atual;
- Armadilha do custo investido: decisões que tentam levar em conta as perdas do passado, mesmo que sejam irrecuperáveis;
- Armadilha da evidência confirmada: decisões baseadas em evidências não confirmadas mas assumidas de forma polêmica;

- Armadilha das tabelas comparativas: um mesmo problema representado por tabelas ou árvores de decisão de modo diferente, dependendo do ponto de vista;
- Armadilha da estimativa e da previsão: valores adotados para estimar um valor ou uma previsão analisados e discutidos para minimizar o efeito do julgamento subjetivo ou superficial;
- Armadilha do excesso de confiança/prudência: podem levar a exageros na obtenção da informação ou decisão.

Estes autores sugerem recorrer ao processo de análise de sensibilidade para avaliar as alternativas de soluções obtidas e a variação dos valores envolvidos. Poder-se-ia acrescentar ainda os seguintes problemas:

- Ignorância: nem tudo é conhecido nem todas as informações necessárias estão disponíveis;
- Conflito: de objetivos, de idéias, de preferências etc.;
- Ambigüidade: de interpretação do problema, de idéias etc.

Neste sentido, decisão deve ser entendida como um processo que deve ser reavaliado sempre que houver necessidade de intervenção para minimizar riscos e erros. O objeto da administração do risco e da tomada de decisão não é nada mais que a busca do equilíbrio entre a medição e a emoção [4].

Discussão e Conclusões

O processo de análise de risco muitas vezes é utilizado para subsidiar decisões estratégicas de uma organização.

No contexto da Auditoria de Sistemas, a análise de risco é referência, quando não o ponto de partida, para promover a adequação na utilização de recursos humanos, materiais e tecnológicos envolvidos no ambiente de sistemas de informação, com vistas a garantir a disponibilidade das operações e serviços, a integridade de dados e informações bem como a confidencialidade das mesmas.

Além disso, o processo de análise de risco possibilita uma melhor administração de riscos, haja vista que avalia impactos, probabilidades de ocorrência, entre outros itens. Administrar, em sentido amplo e geral, está relacionado com escolhas, ou melhor, decisões, e se existem modelos e processos de decisão que visam solucionar problemas com eficácia e/ou eficiência, é possível que estes também possam ser estudados e analisados quanto à utilização em processos de análise e administração de risco.

- Como maximizar os objetivos da organização a partir de soluções ótimas ?
- Se soluções ótimas não são possíveis de serem alcançadas, como lidar com soluções que satisfaçam o problema ?
- É possível ignorar um problema em função de outro ?
- Como e a partir de que parâmetros as ações devem ser priorizadas ?
- Como trabalhar com situações de decisão que envolvem mais de uma pessoa e de níveis hierárquicos e perfis de risco diferentes ?

Os modelos de decisão, quando aplicados a situações de trabalhos de auditoria de sistema certamente não significam que as decisões serão decorrentes de processos infalíveis ou perfeitos. Tampouco significa que não serão encontrados erros mesmo após uma decisão considerada como solução ótima.

Seja qual for o modelo e o processo de decisão adotado, cabe salientar que ainda assim, um mesmo processo de análise de risco, para atender os propósitos de trabalho de auditoria de sistemas, pode contemplar um ou mais modelos e processos para cada ponto de controle ou de auditoria avaliado.

O uso de ferramentas informatizadas específicas para análise de risco podem sim, auxiliar e facilitar a resolução de problemas mais complexos, e requer o conhecimento de algumas condições do processo de decisão preliminarmente, tais como o tipo de abordagem do problema (se analítico, abrangente, estruturado etc.), se trata-se de um problema que envolve ambigüidade, se requer tratamento para dados quantitativos e qualitativos (subjetivos) etc. Requer, acima de tudo, conhecer, mesmo que limitadamente, com que tipos de modelos de decisão ele (software) deve trabalhar. E é nesse sentido que se coloca que é desejável que a decisão esteja apoiada em um processo formal ou, ao menos, em um modelo claro de avaliação e decisão.

O importante é que esses modelos traduzam uma leitura mais pragmática da realidade de tomada de decisões e tornem mais objetivo o processo de decisão; e a decisão, por sua vez, leve em consideração, tanto a intuição inventiva quanto a lógica (raciocínio lógico).

Referências

[1] ARIMA, C. H. **Metodologia de auditoria de sistemas**. São Paulo: Érica, 1994.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação: Código de prática para a gestão da segurança da informação: NBR ISO/IEC 17799:2005**. São Paulo: ABNT, 2005.

[3] ATTIE, W. **Auditoria: conceitos e aplicações**. 2ª ed., São Paulo: Atlas, 1984

[4] BERNSTEIN, P. L. **Desafio aos deuses: a fascinante história do risco**. 10ª ed. Rio de Janeiro: Campus, 1997.

[5] BRODER, J. F. **Risk Analysis and The Security Survey**. Butterworth-Heinemman, 1999.

[6] CIECHANOWICZ, Z. **Risk analysis: requirements, conflicts and problems**. Computers & Security. v. 16, nº 3, p.223-232, 1997.

[7] COOPER, D. R., SCHINDLER, P. S. **Métodos de Pesquisa em Administração**. 7ª ed. Porto Alegre: Bookman, 2003.

[8] DIAS, C.. **Segurança e auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

[9] GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1994.

[10] HOY, W. K., TARTER, C. J. **Administrators solving the problems of practice: decision-making concepts, cases and consequences**. 2 ed. Allyn and Bacon, 1995.

[11] KAUFMANN, A. **A ciência da tomada de decisão: uma introdução à praxiologia**. 2ª. ed. Rio de Janeiro: Zahar Editores, 1981.

[12] NOSWORTHY, J. D. **A practical risk analysis approach: managing BCM risk**. Computers & Security. v. 19, nº 7, p.596-614, 2000.

[13] SELLTIZ, C., JAHODA, M., DEUTSCH, M., COOK, S. M. **Método de Pesquisa das Relações Sociais**. São Paulo: Herder, 1965.

[14] SHIMIZU, T. **Decisão nas organizações: introdução aos problemas de decisão encontrados nas organizações e nos sistemas de apoio à decisão**. São Paulo: Atlas, 2001.

Contato

Cristiane Yayoko Ikenaga
Rua Machado Bittencourt, 361 – conj. 902, V. Clementino, S. Paulo – SP CEP 04044-001
Tel: 55 11 5085-5828
E-mail: **Cristiane@arimaconsulting.com.br**