

Risk IT Based on COBIT: Uma visão sistêmica para a auditoria de TI
Elias Ferreira do Nascimento Neto, CISA, CRISC
elias.neto@audicaixa.org.br

Luiz Claudio Diogo Reis, CISA, CRISC, MCSO
lcdreis@audicaixa.org.br

Não existe uma coisa chamada risco de TI.
Jay Taylor, Diretor Geral de Auditoria de TI da General Motors.

1 Introdução

O dicionário eletrônico Houaiss da Língua Portuguesa define “risco” como a probabilidade de insucesso de determinado empreendimento, em função de acontecimento eventual, incerto, cuja ocorrência não depende exclusivamente da vontade dos interessados.

A preocupação com os riscos não é uma novidade: desde os raios que fizeram com que os homens procurassem abrigo aos modernos sistemas de segurança e defesa nacionais, o desejo de se proteger ou tentar diminuir as consequências da incerteza fez parte da natureza humana.

Essa preocupação, atualmente, está mais em evidência por conta de acontecimentos recentes na história como o “onze de setembro”, por exemplo, o processo de globalização, questões ecológicas e climáticas que afetam a própria possibilidade de sobrevivência de nossa espécie; e, não menos importante, a afluência da sociedade do conhecimento, fatos que colaboram para que cada vez mais haja uma maior preocupação com a questão do tratamento de riscos.

Nesse estado de “coisas”, as organizações têm procurado estabelecer diretrizes e políticas que procuram resguardar seus interesses e buscam alternativas para melhorar cada vez mais o gerenciamento de risco sem oferecer detrimento às suas missões, seja pela busca do lucro, para as entidades privadas ou para atendimento aos cidadãos ou outros fins ligados ao bem público, para as organizações públicas. De qualquer forma, todas estão cada vez mais preocupadas em atender às demandas de seus *stakeholders*.

Segundo CASTELLS (2003), vivemos na Sociedade da Informação e do Conhecimento (*Knowledge Society*) na qual:

O termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo entre indústria e industrial. Uma sociedade industrial não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas da atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos sociedade informacional e economia informacional tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades. (CASTELLS 2003: 65).

A seguir, CASTELLS (2003) explica:

“O que caracteriza a revolução tecnológica atual não é o caráter central do conhecimento e da informação, mas a aplicação deste conhecimento e informação a aparatos de geração de conhecimento e processamento da informação/comunicação, em um círculo de retroalimentação acumulativa entre a inovação e seus usos”. E observa: “A difusão da tecnologia amplifica infinitamente seu poder ao se apropriar de seus usuários e redefini-los. As novas tecnologias da informação não são apenas ferramentas para se aplicar, mas processos para se desenvolver. (CASTELLS 2003: 69) Pela primeira vez na história, a mente humana é uma força produtiva direta, não apenas um elemento decisivo do sistema de produção”.

Para DAVENPORT (1998), a continuidade das organizações é influenciada e determinada em função do seu desempenho na condução dos recursos informacionais. Todavia, os sistemas de informações das organizações foram construídos ao longo dos últimos cinquenta anos de forma atabalhoada e isolada, o que propiciou o crescimento e multiplicação de dados de forma desordenada até atingir o ponto de problemas de gestão, crescimento e dificuldades para promoção da sua inovação e integração.

A situação atual é a seguinte: existe muita informação, espalhada e de difícil integração; existem poucos dados que possam se recuperados e utilizados com a confidencialidade, integridade e disponibilidade necessárias para desempenho das tarefas da gestão, o que afeta o desempenho da organização numa economia altamente competitiva.

Nesse contexto, a busca de soluções de otimização dos poucos recursos existentes, melhorias de controle e propagação de informações confiáveis, que aumentam a transparência e diminuam os problemas enfrentados pelos administradores é premente e, a gestão de riscos informacionais ou de TI, que tratamos a seguir, torna-se cada vez mais desejável, senão imprescindível para a perenidade das organizações.

2 Process Frameworks

Entre essas soluções, a adoção de “*frameworks*” de processo para tratar esses desafios vem sendo, nos últimos anos, uma das abordagens mais frequentes adotadas pelas organizações. A palavra “*framework*”, cuja tradução mais apropriada para o nosso contexto seria “estrutura lógica”, vem sendo usada há muitos anos no ambiente de negócios, mas ainda carece, no contexto da auditoria de TI, de uma definição comum quando a utilizamos.

Por exemplo, segundo a ISACA, o COBIT é um “*framework*” de processo (ver Cobit 4.1), mas não há uma definição precisa do que seria efetivamente um “*process framework*”. O glossário da entidade (<http://www.isaca.org/Pages/Glossary.aspx?tid=4225&char=F>, consultado em 28 SET 11) registra as expressões “*control framework*”, e “*IT governance framework*”, as quais adaptamos para considerar que um *framework* de processo é um modelo que integra uma série de guias, políticas e métodos que representam uma determinada abordagem a um determinado assunto.

3 Frameworks de Gerenciamento de Risco

Os principais *frameworks* de processo que tratam diretamente de gestão de risco estão registrados na tabela abaixo:

Framework	Descrição
COSO	Focado em controles internos das organizações.
COSO ERM (COSO II)	Evolução do COSO, incorporando o processo de gerenciamento de risco.
FERMA	Norma europeia para gerenciamento de risco.
AS/NZS4360	Norma australiana e neozelandesa para tratamento de riscos em sistemas de informação, resultante de uma longa evolução que começou em 1995, cuja versão atual foi publicada em 2004.
ISO 31000	Promove uma linguagem e um modelo comum para ser usado em organizações que implantam um modelo de gerenciamento de risco que busca a consistência, a replicação e a acurácia.
Management of Risk: Guidance for Practitioners (M_o_R)	Guia britânico publicado originalmente em 2004 e que teve uma nova versão lançada em 2007, com foco nas seguintes áreas de gestão de risco: princípios, abordagem, processos, integração e revisão contínua.

Fonte: Adaptado de Risk Management Standards - Role, benefits & applicability, Erben

A necessidade do tratamento específico de determinados assuntos que, ao longo dos anos, vem ficando cada vez mais complexos ensejou o desenvolvimento de *frameworks* de processos que hoje são de conhecimento comum, com focos específicos, tais como:

Framework	Foco em
ISO 27002	Segurança da Informação
COBIT	Controles de processos de TI
VAL IT	Obtenção de valor para a TI
<i>RISK IT</i>	Tratamento dos riscos de TI
Basiléia I e II	Tratamento dos riscos de Instituições Financeiras
PMBOK	Gestão de Projetos

4 Framework *RISK IT*

Risco de TI é o risco do negócio associado com o uso, a propriedade, a operação, o envolvimento, a influência e a utilização de recursos de TI nas organizações e que se caracteriza por eventos de TI (*IT related events*) que podem impactar o negócio, que se relaciona pela incerteza (frequência e magnitude) e, por fim, cria desafios para o atingimento de metas e objetivos do negócio.

O *framework RISK IT* menciona três categorias de risco de TI: a primeira está relacionada à entrega de serviços de TI e diz respeito à área de operações, no que tange ao desempenho, disponibilidade, *compliance* e segurança das atividades diárias: “Manter TI”; a segunda trata da entrega das soluções de TI e em conexão aos programas e projetos da organização, tendo como componentes as oportunidades de negócio, investimento, custo, prazo e escopo: “Desenvolver TI”; e, por fim, a terceira categoria é a dos benefícios e valor para a TI, na qual se analisam os riscos envolvidos na área de negócio, eficiência e eficácia e busca a melhoria de processos: “Pensar TI”.

Jay Taylor, diretor de Auditoria de TI da General Motors, entende que não existe o risco de TI, visto que esse risco está sempre associado a um risco corporativo de negócio, que pode ser de natureza ambiental, organizacional, de mercado, dentre outros.

Assim, o risco de TI refere-se aos riscos corporativos que serão gerados se os serviços de TI não forem entregues (operação de TI), se novas soluções que aproveitam oportunidades de negócio não forem concretizadas (desenvolvimento de TI) ou se não houver benefícios para a organização gerados por TI (valor de TI).

4.1 Princípios do Risk IT

Fischer, em sua série de artigos “*Identify, Govern and Manage IT Risk*” publicados no ISACA Journal, vol. 4, 5 e 6 de 2009, analisa que o *framework Risk IT* está fundamentado em princípios para a gestão efetiva do risco de TI que possuem lastro em outros princípios geralmente aceitos para o gerenciamento do risco, como COSO ERM e a ISO 31000. Essas estruturas foram adaptadas para sua aplicação no domínio da TI, sendo os princípios do RISK IT relacionados a:

- ✓ Governança do Risco de TI;
- ✓ Alinhamento aos riscos do negócio;
- ✓ Alinhamento da gestão dos riscos de TI à gestão de riscos da organização;
- ✓ Realização de análise de custo/benefício do gerenciamento de riscos;
- ✓ Efetivação do gerenciamento de risco da organização;
- ✓ Promoção da comunicação aberta e honesta do risco de TI;
- ✓ Estabelecimento de estrutura de responsabilidade pelas operações por meio de níveis aceitáveis e bem definidos de tolerância a risco; e
- ✓ Promoção do gerenciamento do risco de TI como um processo diário e contínuo na vida da organização.

4.2 Domínios do Risk IT

Buscando auxiliar o atingimento desses objetivos, o *framework Risk IT* foi estruturado em três domínios que abarcam os processos a serem tratados para a concretização da gestão dos riscos de TI, conforme a seguir:

4.2.1 Domínio Governança do Risco

Tem por objetivo certificar que as práticas de gerenciamento de risco estão incorporadas na organização, permitindo-lhe assegurar um retorno aceitável do risco ajustado. Este domínio atua em três processos: o estabelecimento de uma visão comum de risco entre negócio e TI, a integração do risco de TI ao risco de negócio da organização e a busca da efetivação de decisões conscientes sobre os riscos de TI.

4.2.2 Domínio Avaliação de Risco

Tem por objetivo assegurar que os riscos de TI relacionados às oportunidades de negócio são identificados, analisados e representados em termos de negócio e busca melhorar essa prática por meio de ações de coleta de dados, análise de riscos e a manutenção de um perfil/apetite de risco de TI da organização.

4.2.3 Domínio Resposta ao Risco

Tem por objetivo assegurar que os requisitos do risco de TI, as oportunidades e os eventos são abordados de forma razoável em relação ao custo/benefício, considerando as prioridades de negócios e seus processos, a articulação do risco, seu gerenciamento e a resposta ao risco.

Por meio dessa estrutura podem ser obtidos os seguintes ganhos para o negócio: atingimento de uma visão acurada dos riscos atuais e futuros relacionados a TI; direcionamento do tratamento de riscos relacionados a TI (macro/micro processos) para além das medidas técnicas de controle e segurança; integração das estruturas de risco e

de *compliance* da organização (negócio) com os riscos de TI; melhoria do relacionamento entre a Alta Administração, CIO e a área de gestão de risco da organização e, a ainda entre os auditores e a gerência; promoção da responsabilidade sobre o risco e sua aceitação por toda a empresa; e, por fim, melhoria nos recursos da organização (custo x benefício).

4.3 Fatores Críticos de Sucesso e o Papel da Auditoria de TI

A gestão dos riscos de TI leva em conta uma gama de fatores críticos de sucesso para sua implantação, tais como o engajamento das pessoas-chave (Negócio e TI), delegação da gestão do risco (responsabilidades), medidas de desempenho e gestão integrada.

É importante entender que o gerenciamento do risco de TI é um processo iterativo, perpétuo e em constante mudança e devem contemplar a definição clara de políticas e procedimentos associados ao processo, englobando decisões sobre investimento, projetos e mudanças no ambiente de TI.

Tais atividades devem estar submetidas a avaliações de riscos feitas por indivíduos autorizados, de forma a criar uma cultura consciente de risco. A criação de uma cultura de risco depende das pessoas que dela participam e, no caso da gestão efetiva do risco de TI, os participantes vão desde os escalões mais altos da organização (executivos e diretores), passando pelos gerentes e profissionais das áreas de risco e os auditores de TI, pois o engajamento de todos nesse processo é fundamental para a concretização da gestão efetiva dos riscos de TI.

Por exemplo, no caso dos auditores de TI, para a área de auditoria interna da organização, a gestão de riscos envolve várias atividades nas quais há a oportunidade de participação e troca de experiências entre os processos de gestão e controle, abrangendo a definição de responsabilidades, objetivos e análises referentes ao apetite e tolerância ao risco, além da avaliação do processo de identificação, análise e a monitoração da exposição ao risco.

A participação da auditoria da TI na construção dessa cultura, desde que mantida a sua independência, pode trazer dividendos extraordinários para a organização e melhoria nos resultados de negócios, pois uma empresa que conhece e trabalha seus riscos de maneira eficiente e eficaz melhora a sua imagem diante do mercado e aumenta a confiança de seus *stakeholders*, alavancando seus resultados.

5 Conclusão

O tratamento do risco é uma prioridade para as organizações, sejam públicas ou privadas, que devem buscar estabelecer diretrizes e políticas de tratamento de risco para melhorar seu gerenciamento na atual Sociedade da Informação e do Conhecimento.

Para tanto, as organizações buscam soluções de otimização e melhorias e por isso as diversas instituições nacionais e internacionais têm desenvolvido e adotado "*frameworks*" de melhoria de processos, para diversos assuntos.

Nesse contexto também foram evoluídos "*frameworks*" específicos (VAL IT, PMBOK, COBIT, ISO 27002) e, entre esses, o *Risk IT* voltado para a melhoria dos processos de governança do risco de TI.

A estruturação do *Risk IT* nos domínios Governança, Avaliação e Resposta ao Risco tem como objetivo, em seu conjunto, direcionar o tratamento de riscos relacionados a TI (macro/micro processos) para além das medidas técnicas de controle e segurança, possibilitando atuar na integração das estruturas de risco e de *compliance* da organização (negócio) com os riscos de TI, com vistas à melhoria da governança de TI da empresa.

Assim, a auditoria de TI, como parte interessada no processo de gestão e controle do ambiente de TI, pode-se utilizar do *framework RISK IT* como um insumo para a melhoria da gestão de risco corporativo da organização, em especial aqueles relacionados aos riscos de TI.

6 Referências Bibliográficas:

- CASTELLS, Manuel. *Sociedades em Redes*. São Paulo: Editora Paz e Terra, 2003;
- DAVENPORT, Thomas H. *Ecologia da informação: por que só a informação não basta para o sucesso na era da informação*. São Paulo: Futura, 1998.
- The Risk IT framework, ITGI, ISACA, 2009;
- Identify, Govern and Manage IT Risk - Article: Disponível em: www.isaca.org;
- ABNT ISO/IEC 31000:2009 - Gestão de Riscos;
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission Enterprise Risk Management - Integrated Framework, USA, 2004. Disponível em: www.coso.org;
- Standards Australia, AS/NZS 4360:2004, Australian/New Zealand Standard for Risk Management, Australia, 2004;
- Westerman, G.; R. Hunter; 'IT Risk - Turning Business Threats Into Competitive Advantage', Harvard Business School Press, USA, 2007;
- Assurance Guide, ITGI, ISACA;
- GAIT for Business and IT Risk (GAIT-R), IIA, 2008;