# Conceptualização do Risco Operacional - Contributos para as Forças Armadas

Doutor
António Carvalho Brito

Doutor
Gonçalo Morais da Costa

Professora Doutora
Manuela Sarmento

## Introdução

As características genéricas do quadro conceptual actual - dinamismo e mutabilidade sem precedentes a todos os níveis - geram novas formas de complexidade, contradições e paradoxos, que se sucedem a um ritmo elevado.

Face ao exposto, a crescente preocupação das organizações com o risco operacional é um facto. Por outro lado, existe uma tendência inata aos órgãos de gestão para confundirem a tentativa de medição do risco operacional com a gestão do risco operacional (Cagan,

2001). Enquanto que a medição do risco operacional se configura na quantificação deste, a gestão do risco operacional diz respeito à continuidade da organização em termos operativos. Segundo Burchell, Clubb e Hopwood (1985), o risco operacional pode ser encarado como um "valor acrescentado" de experiência.

## Conceptualização do Risco Operacional

O conceito de risco é indissociável da actividade de gestão e afigura-se como crucial, face a um contexto global de elevado dinamismo e mutabilidade, como se caracteriza a realidade actual.

Etimologicamente, a palavra risco deriva do latim *risicare*, cujo significado é ousar. Presentemente a palavra risco configura a probabilidade de um acontecimento apresentar um resultado negativo (com o sentido de perda) num momento futuro. O risco representa alguém ou algo que cria ou sugere um perigo (Peltier, 2001). Porém Lowes (1999), define risco como algo que pode impedir o alcance dos objectivos propostos.

Assumindo, então, o significado da palavra risco, de acordo com Peltier (2001), pode-se dizer que o conceito de escolha surge implicitamente, pelo que é fundamental na gestão de risco.

Para Helland (1998), o risco operacional é a perda potencial causada por uma falha na informação, na comunicação e/ou nos sistemas instituídos. Este risco pode ser mitigado pela manutenção de um sistema de controlos internos.

Pode, ainda, dizer-se que o risco operacional é igual ao controlo dos riscos, adicionado aos riscos inerentes aos controlos ainda estão definidos.

Em qualquer área de negócio, existem sempre riscos inerentes para os quais os controlos não estão devidamente programados, sendo o estabelecimento destes controlos o resultado da análise custo/benefício.
Contudo, os controlos podem ser ineficazes ou podem falhar devido:
- às pessoas:
- aos processos;
- aos sistemas;
- aos eventos externos.

No entanto, os riscos inerentes podem mudar, fruto de alterações no ambiente externo e interno da organização (Bhatia, 2002).

O Comité de Basileia (Bank for International Settlements, 2004) define risco operacional como o risco de perda, que resulta de uma inadequação ou fracasso dos processos internos, das pessoas e dos sistemas, ou de eventos externos. O Comité referencia que

esta definição exclui o risco sistémico, o risco legal e o risco de reputação.

De facto, o risco operacional é uma forma conveniente de capturar todos os tipos possíveis de riscos existentes. Existem duas categorias latas de risco operacional:
- o risco operacional externo;
- o risco operacional interno (Ong, 2002).

O termo genérico "risco operacional" foi oficialmente introduzido, em 1991, pelo relatório do *Committee of Sponcering Organizations of the Treadway Commission* (COSO, 1992). Contudo, quando, em 1996, um fogo destruiu o *Crédit Lyonnais*, categorizou-se a perda do ponto de vista do risco operacional na categoria de fogos, mas os investigadores suspeitaram que tivesse havido um fogo posto pelos colaboradores do Banco, com o intuito de destruir as evidências de fraudes que tinham sido praticadas.

Foi com base neste incidente, que o Comité de Basileia esboçou um documento, o *Sound Practices for the Management and Supervision of Operational Risk* (Bank of International Settlements, 2003), onde evidenciava as melhores práticas para a gestão do risco operacional. Este documento deve ser encarado como uma tentativa conjunta de esforços dos académicos e dos órgãos de gestão de risco das principais instituições financeiras.

O documento defende que o planeamento global, a coordenação e a monitorização do risco operacional devem estar centralizados num departamento denominado "gestão do risco".

As competências deste departamento são de coordenação dos riscos de mercado e de crédito, no âmbito de uma gestão global dos riscos, no seio das organizações.
As contingências podem assumir duas categorias latas:
- as contingências que ocorrem frequentemente e dão origem a perdas tidas como modestas;
- as contingências que não ocorrem frequentemente, mas que podem gerar perdas significativas.

Ainda, de acordo com o documento em causa, a gestão do risco operacional deveria combinar técnicas qualitativas e quantitativas, para uma correcta avaliação dos riscos. Outras contingências de difícil modelação, que afectam as instituições financeiras, são as que não ocorrem de uma forma frequente e cuja natureza não é uniforme. Exemplos disso são os actos de terrorismo, os desastres naturais e as fraudes. Segundo Cruz (2002) as técnicas de medição dividem-se em dois grandes grupos:

- técnicas qualitativas;
- técnicas quantitativas.

O documento designado Basileia II, que foi apresentado em Janeiro de 2001, é consultivo e inclui um conjunto de documentos de análise de risco e gestão do risco (Bank for International Settlements, 2001a).

Uma extensa avaliação que foi feita pelo sector bancário, leva posteriormente o comité a publicar um novo documento em Setembro de 2001, referente ao risco operacional (Bank for International Settlements, 2001b).

Subsequentemente, em Abril de 2003, é novamente revisto o documento de Basileia II. Finalmente, em 2004, é apresentado o acordo final de Basileia II (Bank for International Settlements, 2004).

No entanto, a tentativa contínua de melhorar a regulamentação prossegue por parte das entidades reguladoras. Daí estar em estudo no *Bank for International Settlements* (BIS) um novo acordo de Basileia, a ser implementado em 2007 (Imeson, 2003).

Para as denominadas contingências operacionais, duas formas de dados são úteis:
- dados históricos sobre eventos que geraram perdas;
- dados referentes a indicadores de risco.

Os eventos resultantes em perda podem dar origem a uma série de falhas dos sistemas, fraudes insignificantes e processos legais a clientes. O âmbito da perda pode ser directo (como no caso de roubo) ou indirecto (como no caso de danos para a reputação da instituição).

No contexto actual, existem três formas de categorizar os dados referentes a eventos, que pressupõem perda:

- evento;
- causa simples ou múltipla;
- consequência simples ou múltipla.

A construção de uma matriz de eventos permite vislumbrar as três dimensões de eventos, que resultam em perda, com o intuito de identificar a frequência com que certas causas são associadas a eventos específicos e consequências associadas. Mesmo sem uma análise adicional, estas matrizes conseguem identificar, nomeadamente as melhorias nos procedimentos e na formação dos colaboradores, entre outras.

O comité de Basileia II evidencia sete categorias gerais de eventos, que propiciam perda, conforme se apresenta na Tabela 1.

# A Aplicação do Risco Operacional às Forças Armadas

A primeira organização que desde sempre lidou com a problemática do risco foram as Forças Armadas. Em termos das operações militares configuram-se três diferentes itens propiciadores de risco:

- a tecnologia;
- os recursos humanos;
- o “cenário” de guerra.

Ao longo da história recente podem-se enumerar vários conflitos, onde o risco operacional emergiu fruto da tecnologia, como por exemplo, na Somália quando os sensores e as tecnologias de recolha e processamento de informação não foram suficientes para o sucesso da missão (McMaster, 2003).

A superioridade da informação não significa informação perfeita (McMaster, 2003). Além do mais, as lições a retirar dos conflitos recentes demonstram que a dependência dos Exércitos, face à tecnologia propiciam claramente um incremento do risco operacional. Daí que, deverá ser desenvolvido um esforço por parte dos Exércitos, de modo a terem capacidade de operar com sistemas tecnológicos menos sofisticados, integrando a componente humana em substituição da tecnológica.

No que diz respeito aos recursos humanos, considera-se que são claramente o elemento que mais contribui para aumentar o risco, devido à complexidade da natureza humana. Na realidade, os factores motivadores e o stress decorrente do conflito são apenas alguns dos motivos causadores de perdas, pelo que existe uma nítida necessidade de se compreender o factor humano.

No entanto e apesar de todos os problemas que se podem evidenciar, tem-se a consciência de que cada vez mais serão os recursos humanos a fazer a diferença, independentemente de ser no “cenário de guerra” ou na organização.

Jiang Zemin (2005) reflecte esta realidade, ao afirmar que a guerra do Iraque provou uma vez mais, que em condições altamente tecnológicas, o factor determinante do resultado da guerra é ainda baseado nas qualidades humanas.

Relativamente ao “cenário” de guerra, este incorpora igualmente valências próprias, atendendo à multiplicidade de factores que daí podem advir. A localização geográfica com todas as suas inerências, desde as variáveis climáticas, às condições do terreno e até às populações locais podem ser factores indiciadores de risco operacional, assim como, o tipo de conflito. Um exemplo actual diz respeito ao conflito no Iraque, onde a cultura islâmica, a população local e a guerrilha são factores geradores do risco.

## A gestão do Risco Operacional no Exército americano

Em 1991, o Exército norte-americano adoptou formalmente uma metodologia de gestão do risco operacional, com o intuito de minimizar os danos decorrentes da sua operacionalidade, após a apresentação do relatório do *Naval Safety Center* (1991) sobre

a guerra no Golfo Pérsico. Este relatório expunha as perdas humanas e materiais, não só resultantes da guerra do Golfo, mas também as decorrentes de outros "palcos de guerra", onde o Exército norte-americano tinha actuado. Para além desta importante informação demonstrava-se ainda o custo financeiro associado a estas perdas.

Seguidamente apresenta-se na Tabela 2 a percentagem de perdas humanas e materiais na Segunda Guerra Mundial, na Guerra da Coreia, na Guerra do Vietname e na Guerra do Golfo.

Na Tabela 3 apresenta-se discriminadamente a categoria das perdas humanas durante a guerra do Golfo.

Na Tabela 4 registam-se os custos financeiros em milhares de dólares, durante a guerra do Golfo.

Contudo, é de realçar que o modelo de gestão do risco operacional adoptado na Guerra do Golfo seguiu a metodologia da Federal Aviation Association (FAA).

A Figura 2 ilustra os objectivos do processo de gestão do risco operacional, nomeadamente *a protecção dos colaboradores, dos equipamentos e outros recursos*, enquanto a organização faz o seu uso efectivo. *A prevenção de acidentes e a tentativa de reduzir as perdas* é um aspecto importante do objectivo enumerado anteriormente. Por seu turno, minimizando-se o risco de dano e perda, a organização é premiada com uma redução de custos. Assim, a meta fundamental da gestão de risco é aumentar a efectividade dos colaboradores e equipamentos determinando-se a fórmula que permita um uso mais eficaz.

Os quatro princípios determinantes das acções associadas à gestão do risco operacional são continuamente empregues, sendo aplicáveis antes, durante e no final de todas as tarefas e operações, por indivíduos pertencente a todos os níveis de responsabilidade hierárquica. Não é aceite nenhum risco desnecessário, atendendo a que não é possível estimar um retorno comensurável, em termos de benefícios ou oportunidades. De facto, as escolhas mais lógicas para a realização de uma operação são as que satisfazem todas as exigências, com um risco mínimo aceitável.

O corolário deste axioma baseia-se num dogma: *aceitar o risco necessário*, exigido para completar a operação ou tarefa com sucesso, tomando-se as decisões de risco ao nível hierárquico apropriado, pois qualquer indivíduo pode tomar uma decisão de risco. Porém, o indivíduo que deve ter os recursos para reduzir ou eliminar o risco e implementar controlos é sempre o líder (Federal Aviation Association, 2000).

Até mesmo comportamentos conotados com riscos elevados podem ser executados, desde que haja um conhecimento claro de que a soma dos benefícios excede a soma dos custos. A análise custo/benefício é indubitavelmente um processo de cariz subjectivo, e em última análise a homeostase pode ser determinada arbitrariamente pelos órgãos de gestão, havendo a integração do planeamento do risco operacional em todos os níveis

hierárquicos - sendo avaliados os riscos mais fáceis de gerir nas fases de planeamento de uma operação. Em termos temporais, as mudanças posteriormente executadas ao longo do processo de planeamento e de execução de uma operação, irão revelar-se mais dispendiosas para a organização. De acordo com a Federal Aviation Association (2000), o processo de gestão do risco operacional inclui seis passos, todos igualmente importantes. A Figura 3 ilustra esses passos:

(1) identificação do perigo,
(2) avaliação dos riscos,
(3) análise dos procedimentos de controlo do risco,
(4) criação de decisões de controlos,
(5) implementação de controlos,
(6) supervisão e revisão.

A avaliação do risco diz respeito à aplicação de medidas quantitativas e qualitativas para determinar o nível de risco associado aos perigos específicos. Este processo define a probabilidade e severidade de um acidente, que poderia ser o resultado dos perigos. Por outro lado, a análise dos procedimentos de controlo do risco investiga as estratégias específicas e as ferramentas que reduzem, mitigam ou eliminam o risco. Pode-se, então, estabelecer que todos os riscos têm três componentes:

- a probabilidade de ocorrência;
- a severidade do perigo;
- a exposição das pessoas e dos equipamentos face ao risco.

Medidas de controlo efectivas reduzem ou eliminam pelo menos um destes.

A análise deverá ter em linha de conta os custos globais e os benefícios decorrentes das acções remediadoras, enquanto mune os órgãos de gestão, se possível, de escolhas alternativas.

No que concerne à criação de decisões de controlos, deverá haver uma clara identificação do decisor. Cabe a este a escolha do controlo ou a combinação das ferramentas que melhor controla o risco. Por outro lado, a gestão tem de formular um plano de aplicação dos controlos, que foram seleccionados. Estando, então, os controlos em funcionamento, o processo deverá ser periodicamente reavaliado, de forma a assegurar a efectividade dos mesmos. Os colaboradores e os órgãos de gestão de todos os níveis hierárquicos têm que cumprir os seus respectivos “papéis organizacionais”, de modo a assegurar que os controlos sejam mantidos com o decurso do tempo.

O processo de gestão do risco prossegue ao longo do ciclo de vida do sistema, da missão ou da actividade. Todo o processo de análise do risco e criação de possíveis controlos assenta na utilização de um questionário a todos os departamentos, o qual se apresenta na Figura 4.

Contudo, após os acontecimentos de 11 de Setembro de 2001, tornou-se claro que novas

medidas e estratégias seriam necessárias, tal como referido pelo Departamento de Defesa dos EUA (Department of Defense, 2001).

Aliás, decorrente deste evento surgiu um documento relativo a futuras estratégias, de forma a gerir o risco operacional. Nesse documento define-se como um dos objectivos primordiais, a criação de uma nova metodologia de gestão do risco operacional, tendo por base quatro valências fundamentais (Department of Defense, 2001):

- *a gestão do risco associado aos recursos humanos*, que trata das questões relacionadas com a capacidade de recrutamento, de treino e de manutenção dos recursos humanos, de modo a que haja uma retenção suficiente de pessoas qualificadas, para as diferentes questões de índole operacional;

- *o risco operacional* que está relacionado com os objectivos militares, num determinado conflito ou noutra contingência de cariz não militar;

- *o risco inerente a desafios futuros* que incorpora as questões relacionadas com o desenvolvimento de novas tecnologias e de inovações organizacionais, que possam minimizar o risco operacional do Exército americano a longo prazo;

- *o risco institucional* que resulta de factores que afectam o desenvolvimento de práticas de gestão do risco e a criação de controlos, que utilizem os recursos eficazmente e promovam a operação efectiva do Exército.

# Conclusão

A metodologia de gestão do risco seguida pelo Exército norte-americano demonstrou, face à Segunda Guerra Mundial, à Guerra da Coreia, à Guerra do Vietnam, à Guerra do Golfo e à Guerra do Iraque que há falhas, pelo que importa que as chefias militares prestem uma forte atenção, de modo a reduzir substancialmente o risco de perdas humanas.

No entanto, este processo necessita de uma perspectiva correcta da realidade, sendo fundamental incorporar contributos de áreas diversas, mesmo de *outsiders*, os quais poderão, em nosso entender, ser sensíveis a um conjunto diferente de sinais. Estes sinais podem, desde sempre, ter estado presentes e serem estimadores do risco.

Aliás, actualmente vive-se a fase da *inflexão estratégica*, pois está-se perante a arriscada transição entre a velha e a nova maneira de actuar, nos vários domínios do conhecimento, incluindo na área da Defesa e da Segurança.

Contudo, tal como em qualquer domínio do saber, também a Defesa e Segurança necessitam de uma transformação de mentalidades, por forma a concretizar com sucesso,

o estabelecido no Conceito Estratégico de Defesa Nacional, quando se afirma que as Forças Armadas "devem dispor de uma organização flexível e modular, adequada aos modernos requisitos de empenhamento operacional, conjunto e combinado, privilegiando a interoperabilidade dos meios e, desejavelmente, com capacidades crescentes de projecção e sustentação, protecção de forças e infra-estruturas, comando, controlo, comunicações e informações" (Governo da República Portuguesa, 2003).

De facto, as barreiras culturais e a resistência burocrática à mudança, bem como a escassez de recursos financeiros, materiais e humanos, promovem a necessidade de uma visão estratégica adequada aos problemas de Defesa e Segurança do Século XXI.

## Bibliografia


Bank for International Settlements. 2001a. Basel committee on baking supervision: operational risk. Basel: Bank for International Settlements;

Bank for International Settlements. 2001b. Basel committee on baking supervision: working paper on the regulatory treatment of operational risk. Basel: Bank for International Settlements;

Bank for International Settlements. 2003. Basel committee on baking supervision: sound practices for the management and supervision of operational risk. Basel: Bank for International Settlements;

Bank for International Settlements. 2004. Basel committee on baking supervision: international convergence of capital measurement and capital standards. Basel: Bank for International Settlements;

Bhatia, M. (2002). Operational risk management: emerging frontiers for the profession, Information Systems Audit and Control Association, [em linha]. [referência 27 de Setembro de 2006]. Disponível na Internet: http://www.isaca.org/PrinterTemplate.cfm?Section=Home&Template=/ ContentManagement/ContentDisplay.cfm&ContentID=7304;

Brink, G. (2002). Operational risk: new challenges for banks. New York: Palgrave Publishers;

Burchel, S., Clubb, C. & Hopwood, A. 1985. Accounting in its social context: towards a history of value added in the UK. Accounting, Organizations and Society, 10, 4, 20-24;

Cagan, P. (2001). Standard operating procedures, Eriks.com, [em linha]. [referência de 27 de Setembro de 2006]. Disponível na Internet: http://www.erisk.com/ResourceCenter/Features/SpecialReport BasleIIResou.asp;

Clarke, L. (1999). Mission improbable. Chicago: University Press of Chicago;

Committee of Sponcering Organizations of the Treadway Commission. 1992. Internal control-integrated framework. [S.l.]: Committee of Sponcering Organizations of the Treadway Commission;

Cruz, M. (2002). Modeling, measuring and hedging operational risk. New York [etc.]: John Wiley & Sons;

Department of Defense. 2001. Military transformation: a strategic approach. Department of Defense;

Federal Aviation Association. 2000. Federal Aviation Association system safety handbook. Virginia: Federal Aviation Association;

Governo da República Portuguesa. (2003). Conceito Estratégico de Defesa Nacional, Portal do Governo da República Portuguesa, [em linha]. [referência de 27 de Setembro de 2006]. Disponível na Internet: http://www.portugal.gov.pt/Portal/PT/Governos/Governos_Constitucionais/GC15/Ministerios/MDN/Comunicacao/Outros_Documentos/20030120_MDN_Doc_CEDN.htm;

Helland, E. 1998. Operational risk takes center stage. Wall Street & Technology, 16, 9, 46-50;

Imeson, M. 2003. The risk angle - does operational risk management require banks to change their core systems?. The Banker, 48, 8-10;

Lowes, J.F. 1999. Information systems: how to run a simple risk management workshop. Management Accounting, 77, 7, 44-45;

McMaster, H. (2003). Crack in the foundation: Defense Transformation and the underlying assumption of dominant knowledge in future warfare, US Army War College, [em linha]. [referência de 27 de Setembro de 2006]. Disponível na Internet: http://www.comw.org/rma/fulltext/0311mcmaster.pdf;

Naval Safety Center. 2001. ORM principles. Washington: Naval Safety Center;

Ong, M. 2002. The alpha, beta and gamma of operational risk. The RMA Journal, 85, 1, 34-38;

Peltier, T. (2001). Information security risk analysis. Boca Raton [etc.]: Auerbach Pulications;

Zemin, J. (2005). Annual Report on the military Power of the People's Republic of China, Defense Link, [em linha]. [referência de 27 de Setembro de 2006]. Disponível na Internet: http://www.defenselink.mil/news/Jul2005/d20050719china.pdf.

_____

* Professor de Ciências Empresariais.
** Professora da Academia Militar.
*** Professor da Universidade do Porto.