

ferma



FEDERATION OF  
EUROPEAN RISK  
MANAGEMENT  
ASSOCIATIONS

## NORMA DE GESTÃO DE RISCOS





## Introdução

A Norma de Gestão de Riscos é o resultado do trabalho de uma equipa composta por elementos das principais organizações de gestão de riscos do Reino Unido - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) e ALARM The National Forum for Risk Management in the Public Sector.

Esta equipa procurou, ao longo de um período de consulta prolongado, os pontos de vista de um grande número de organismos profissionais com interesses na gestão de riscos.

A gestão de riscos é uma disciplina em rápido desenvolvimento. Existem diversos pontos de vista, assim como descrições sobre o que engloba, como deve ser conduzida e para que serve. São necessárias normas para garantir uma concordância em relação a:

- *terminologia utilizada,*
- *processos para implementação da gestão de riscos,*
- *estrutura organizacional para a gestão de risco,*
- *objectivo da gestão de riscos.*

Importa referir que esta norma reconhece que o risco apresenta duas vertentes, não só a negativa, mas também a positiva.

A gestão de riscos não é apenas um tema para empresas ou organizações públicas, mas também para qualquer actividade ou projecto de curto ou longo prazo. As vantagens e

oportunidades devem ser vistas não só no contexto da própria actividade, mas também em relação às muitas e diversas partes interessadas que podem ser afectadas, doravante designadas por intervenientes (Stakeholders).

Existem muitas formas de atingir os objectivos da gestão de riscos e seria tarefa impossível tentar defini-las todas num único documento. Por conseguinte, nunca foi nosso objectivo produzir uma norma prescritiva, que conduziria a uma abordagem do tipo lista de verificação, nem estabelecer um processo de certificação. Ao cumprirem as várias componentes desta norma e podendo fazê-lo de formas diversas, as organizações ficarão em posição de informar sobre a sua conformidade com a mesma. A norma representa as melhores práticas em relação às quais as organizações se podem auto-avaliar.

A norma utilizou, sempre que possível, a terminologia para o risco definida pela Organização Internacional de Normalização (ISO) no seu recente documento, ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

Devido aos rápidos desenvolvimentos a que se assiste nesta área, os autores gostariam de receber comentários por parte das organizações que coloquem a norma em prática (as moradas estão indicadas na contracapa deste Guia). Pretende-se que a norma evolua regularmente, à luz das melhores práticas.



## 1. Risco

O risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências (ISO/IEC Guide 73).

O simples facto de existir actividade, abre a possibilidade de ocorrência de eventos ou situações cujas as consequências constituem oportunidades para obter vantagens (lado positivo) ou então ameaças ao sucesso (lado negativo).

A gestão de riscos é cada vez mais identificada como dizendo respeito aos aspectos positivos e negativos do risco. Por conseguinte, esta norma considera o risco nestas duas perspectivas.

No campo da higiene e segurança, por exemplo, é quase um dado adquirido que as consequências são apenas negativas e, por isso, a gestão destes riscos concentra-se na prevenção ou diminuição do dano.

## 2. Gestão de riscos

A gestão de riscos é um elemento central na gestão da estratégia de qualquer organização. É o processo através do qual as organizações analisam metodicamente os riscos inerentes às respectivas actividades, com o objectivo de atingirem uma vantagem sustentada em cada actividade individual e no conjunto de todas as actividades.

O ponto central de uma boa gestão de riscos é a identificação e tratamento dos mesmos. O seu objectivo é o de acrescentar valor de forma sustentada a todas as actividades da organização. Coordena a interpretação dos potenciais aspectos positivos e negativos de

todos os factores que podem afectar a organização. Aumenta a probabilidade de êxito e reduz tanto a probabilidade de fracasso como a incerteza da obtenção de todos os objectivos globais da organização.

A gestão de riscos deve ser um processo contínuo e em constante desenvolvimento aplicado à estratégia da organização e à implementação dessa mesma estratégia. Deve analisar metodicamente todos os riscos inerentes às actividades passadas, presentes e, em especial, futuras de uma organização. Deve ser integrada na cultura da organização com uma política eficaz e um programa conduzido pela direcção de topo. Deve traduzir a estratégia em objectivos táticos e operacionais, atribuindo responsabilidades na gestão dos riscos por toda a organização, como parte integrante da respectiva descrição de funções. Esta prática sustenta a responsabilização, a avaliação do desempenho e respectiva recompensa, promovendo desta forma a eficiência operacional em todos os níveis da organização.

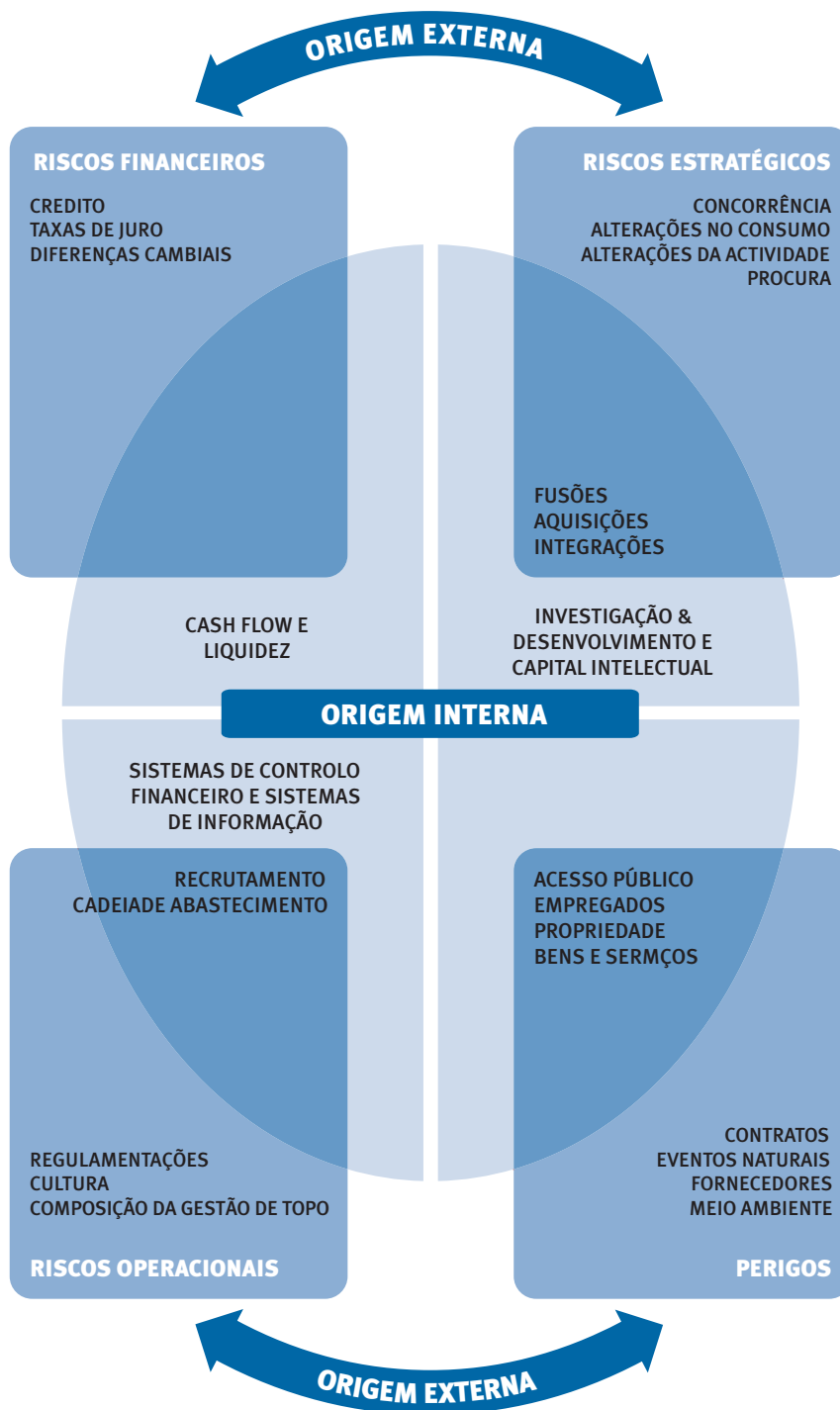
### 2.1 Factores externos e internos

Os riscos que uma organização e respectivas actividades apresentam podem ter origem em factores que podem ser internos ou externos à organização.

O diagrama (2.1.1) propõe exemplos de riscos principais e mostra que alguns deles respondem a factores tanto internos como externos. A classificação dos riscos pode ser ajustada, fazendo a distinção dos mais relevantes de entre os riscos puros e os de ordem estratégicos, financeiros, operacionais, etc.

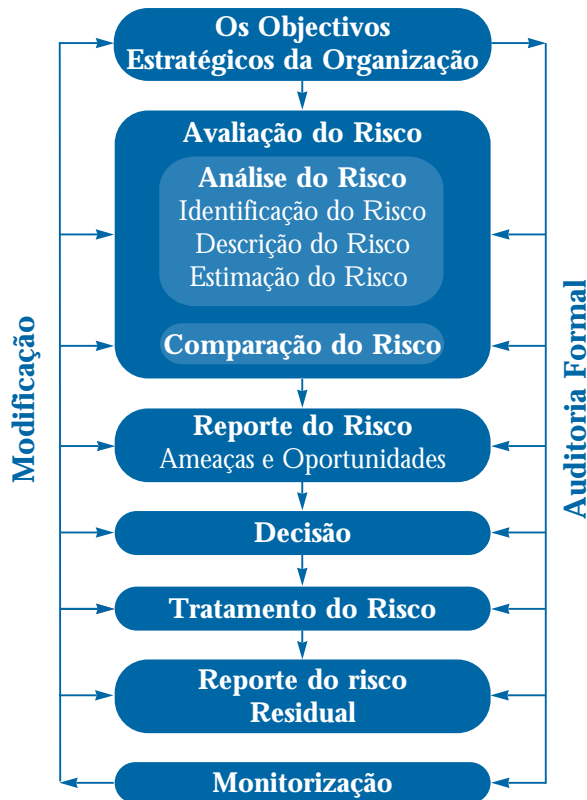


## 2.1 Exemplos de factores internos e externos





## 2.2 Processo de gestão de riscos



A gestão de riscos protege e acrescenta valor à organização e aos diversos intervenientes, apoiando da seguinte forma os objectivos da organização:

- criação de uma estrutura na organização que permita que a actividade futura se desenvolva de forma consistente e controlada
- melhoria da tomada de decisões, do planeamento e da definição de prioridades, através da interpretação abrangente e estruturada da actividade do negócio, da volatilidade dos resultados e das oportunidades/ameaças do projecto
- contribuição para uma utilização/atribuição mais eficiente do capital e dos recursos dentro da organização
- redução da volatilidade em áreas de negócio não essenciais
- protecção e melhoria dos activos e da imagem da empresa
- desenvolvimento e apoio à base de conhecimentos das pessoas e da organização
- optimização da eficiência operacional.



### 3. Avaliação de riscos

A avaliação de riscos é definida pelo documento ISO/IEC Guide 73 como o processo geral de análise de riscos e estimativa de riscos.  
(Consulte o anexo)

### 4. Análise de riscos

#### 4.1 Identificação dos riscos

A identificação dos riscos tem como objectivo identificar a exposição de uma organização ao elemento de incerteza. Esta identificação exige um conhecimento profundo da organização, do mercado no qual esta desenvolve a sua actividade, do ambiente jurídico, social, político e cultural onde está inserida, assim como o desenvolvimento de uma sólida interpretação das suas estratégias e objectivos operacionais, incluindo os factores fundamentais para o seu êxito e as ameaças e oportunidades relativas à obtenção dos referidos objectivos. A identificação dos riscos deve ser abordada de forma metódica, de modo a garantir que todas as actividades significativas dentro da organização foram identificadas e todos os riscos delas decorrentes definidos. Toda a volatilidade associada relativa a estas actividades deve ser identificada e classificada por categorias.

**As actividades e decisões podem ser classificadas de várias formas, entre as quais:**

- *Estratégicas - Relacionadas com os objectivos estratégicos da organização a longo prazo. Podem ser afectadas por áreas como disponibilidade de capital, riscos de soberania e políticos, alterações jurídicas e regulamentares, reputação e alteração ao meio ambiente físico.*
- *Operacionais - Relacionadas com os assuntos quotidianos com os quais a organização é confrontada quando se esforça para atingir os seus objectivos estratégicos.*
- *Financeiras - Relacionadas com a gestão e controlo eficazes dos meios financeiros da organização e com os efeitos de factores externos como, por exemplo, disponibilidade de crédito, taxas de câmbio, movimento das*

*taxas de juro e outro tipo de orientações do mercado.*

- *Gestão do conhecimento - Relacionadas com a gestão e controlo eficazes dos recursos do conhecimento e com a produção, protecção e comunicação destes. Esta categoria engloba factores externos como a utilização não autorizada ou abusiva da propriedade intelectual, as falhas de energia na zona e tecnologia competitiva. Do lado dos factores internos podem referir-se avarias nos sistemas ou a perda de funcionários chave.*
- *Conformidade - Relacionadas com temas como saúde e segurança, meio ambiente, práticas comerciais, protecção do consumidor, protecção de dados, assuntos regulamentares legislação laboral.*

Apesar da identificação dos riscos poder ser realizada por consultores externos, uma abordagem interna com processos e ferramentas bem comunicados, consistentes e coordenados (consulte o anexo) será provavelmente mais eficaz. É essencial que sejam os actores internos os 'proprietários' do processo de gestão de riscos.

#### 4.2 Descrição dos riscos

O objectivo da descrição dos riscos centra-se na apresentação dos riscos identificados num formato estruturado, por exemplo, através de uma tabela. A tabela (4.2.1) de descrição dos riscos pode facilitar a descrição e avaliação de riscos. A utilização de uma estrutura bem concebida é necessária para garantir um processo abrangente de identificação, descrição e avaliação de riscos. Ao considerar-se a consequência e probabilidade de cada um dos riscos definidos na tabela, deve ser possível identificar os riscos chave e estabelecer prioridades na análise detalhada dos mesmos. A identificação dos riscos associados a actividades de negócio pode ser dividida em estratégica, de projecto/táctica, operacional. É importante incorporar a gestão de riscos em toda a fase de vida do projecto, desde a concepção, passando pela execução até à sua conclusão.



#### 4.2.1 Tabela - Descrição dos riscos

|   |  |
|---|--|
| 1. Designação do risco                          |  |
| 2. Âmbito do risco                              | Descrição qualitativa de acontecimentos, como dimensão, tipo, número e dependências  |
| 3. Natureza do risco                            | Ex. estratégicos, financeiros, operacionais, de conhecimento ou conformidade   |
| 4. Intervenientes                               | Intervenientes e respectivas expectativas  |
| 5. Quantificação do risco                       | Importância/relevância e probabilidade   |
| 6. Tolerância/Apetência para o risco            | Potencial de perda e impacto financeiro do risco<br>Valor em risco (value at risk)<br>Probabilidade e dimensão de perdas/ganhos potenciais<br>Objectivo(s) do controlo do risco e nível de desempenho pretendido |
| 7. Tratamento e mecanismos de controlo do risco | Principais meios através dos quais o risco é actualmente gerido<br>Níveis de confiança do controlo existente<br>Identificação dos protocolos de monitorização e revisão  |
| 8. Possíveis acções de melhoria                 | Recomendações para redução do risco  |
| 9. Desenvolvimento de estratégias e políticas   | Identificação da função responsável pelo desenvolvimento de estratégias e políticas  |

#### 4.3 Estimativa dos riscos

A estimativa dos riscos pode ser quantitativa, semi-quantitativa ou qualitativa em termos de probabilidade de ocorrência e possível consequência.

Por exemplo, as consequências em termos de ameaças (riscos de aspectos negativos) e oportunidades (riscos de aspectos positivos) podem ser altas, médias ou baixas (consulte a tabela 4.3.1). As probabilidades podem ser altas, médias ou baixas, mas exigem definições diferentes em relação a ameaças e oportunidades (consulte as tabelas 4.3.2 e 4.3.3).

São fornecidos exemplos nas tabelas apresentadas. Cada organização poderá considerar diferentes metodologias, quer na medição das consequências, quer das probabilidades, adequando-as às suas necessidades. Por exemplo, muitas organizações consideram que avaliar as consequências e probabilidades como altas, médias ou baixas se adequa às respectivas necessidades e podem ser apresentadas numa matriz de 3 x 3. Outras consideram que avaliar as consequências e probabilidades através de uma matriz de 5 x 5 proporciona uma melhor estimativa.



#### 4.3.1. Tabela - Consequências para ameaças e oportunidades

|       |  |
|-------|--|
| Alta  | O impacto financeiro sobre a organização deve ultrapassar os x €<br>Impacto significativo sobre a estratégia ou actividades operacionais da organização<br>Grande preocupação dos intervenientes |
| Média | O impacto financeiro sobre a organização deve ser entre x € e y €<br>Impacto moderado sobre a estratégia ou actividades operacionais da organização<br>Preocupação moderada dos intervenientes   |
| Baixa | O impacto financeiro sobre a organização deve ser inferior a y €<br>Impacto baixo sobre a estratégia ou actividades operacionais da organização<br>Pouca preocupação dos intervenientes          |

#### 4.3.2. Tabela - Probabilidade de ocorrência (Ameaças)

| Estimativa       | Descrição  | Indicadores  |
|------------------|--|--|
| Alta (Provável)  | Com possibilidade de ocorrência todos os anos ou hipótese de ocorrência superior a 25%.    | Potencial para ocorrer diversas vezes dentro do período de tempo (por exemplo - dez anos). Ocorreu recentemente.   |
| Média (Possível) | Com possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 25%. | Pode ocorrer mais do que uma vez dentro do período de tempo (por exemplo - dez anos). Pode ser difícil de controlar devido a algumas influências externas. Existe um historial de ocorrências? |
| Baixa (Remota)   | Sem possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 2%.  | Não ocorreu. Improvável que ocorra.  |



#### 4.3.3. Tabela - Probabilidade de ocorrência (Oportunidades)

| Estimativa       | Descrição  | Indicadores   |
|------------------|--|---|
| Alta (Provável)  | É provável a obtenção de um resultado positivo num ano ou hipótese de ocorrência superior a 75%.   | Clara oportunidade, com certeza razoável, a ser atingida a curto prazo, com base nos processos de gestão actuais.   |
| Média (Possível) | Perspectivas razoáveis de resultados favoráveis num ano ou hipótese de ocorrência entre 25% a 75%. | Oportunidades que podem ser atingíveis, mas exigem uma gestão cuidadosa.<br>Oportunidades que podem surgir para além do plano.  |
| Baixa (Remota)   | Alguma hipótese de resultados favoráveis a médio prazo ou hipótese de ocorrência inferior a 25%.   | Possível oportunidade que ainda deve ser totalmente investigada pela direcção. Oportunidade cuja probabilidade de sucesso é baixa, com base nos recursos de gestão que estão a ser aplicados. |

#### 4.4. Métodos e técnicas de análise de riscos

Podem ser utilizadas diversas técnicas para analisar riscos. Estas técnicas podem ser específicas de riscos com aspectos positivos ou negativos ou podem ter a capacidade de analisar ambos os tipos. *(consulte o anexo para obter exemplos).*

#### 4.5. Perfil dos riscos

O resultado do processo de análise de riscos pode ser utilizado para gerar um perfil dos riscos que classifica cada risco segundo a sua importância e fornece uma ferramenta para

determinar a prioridade dos esforços de tratamento. Este perfil classifica cada risco identificado, de modo a dar uma ideia da sua importância relativa.

Este processo permite atribuir o risco à área de negócio afectada, descreve os principais procedimentos de controlo implementados e indica as áreas onde o nível de investimento no controlo de riscos deve ser aumentado, diminuído ou redistribuído.

A responsabilização ajuda a identificar claramente o 'proprietário' do risco e garantir que lhe são afectados os recursos adequados.



## 5. Comparação de riscos

Quando o processo de análise de riscos estiver concluído, é necessário comparar os riscos estimados com os critérios de riscos definidos pela organização. Os critérios de riscos podem englobar os custos e receitas associados, exigências legais, factores socio-económicos e ambientais, preocupações dos intervenientes, etc. Desta forma, a estimativa de riscos e subsequente comparação apoia na tomada de decisões sobre a importância dos riscos para a organização e sobre a possibilidade de cada risco específico ser aceite ou corrigido.

## 6. Tratamento de riscos

O tratamento de riscos é o processo de seleccionar e implementar medidas para modificar um risco. O elemento principal do tratamento de riscos é o controlo/diminuição dos riscos, mas engloba, num contexto mais vasto, por exemplo, o evitar de riscos, a transferência, o financiamento, etc.

**NOTA:** Nesta norma, o financiamento de riscos refere-se aos mecanismos (ex. programas de seguros) para constituição de fundos para as suas consequências financeiras. De modo geral, não se considera o financiamento de riscos como uma provisão de fundos para suportar os custos da implementação do tratamento de riscos (conforme definido pelo documento ISO/IEC Guide 73; consulte a página 17).

No mínimo, qualquer sistema de tratamento de riscos deve:

- proporcionar um funcionamento eficaz e eficiente da organização
- garantir controlos internos eficazes
- cumprir com leis e regulamentações

O processo de análise de riscos apoia o funcionamento eficaz e eficiente da organização através da identificação dos riscos aos quais a gestão deve prestar maior atenção.

Assim devem ser definidas prioridades nas acções de controlo em termos do seu potencial para benefício da organização.

A eficácia do controlo interno mede-se pelo grau de eliminação ou redução do risco através das medidas propostas.

A eficácia em termos de custos dos controlos internos está relacionada com os custos da sua implementação quando comparados com os benefícios esperados pela redução dos riscos.

**Para avaliar os mecanismos de controlo propostos é necessário medir e comparar:**

- *potencial efeito económico se estes não forem implementados*
- *custos da implementação destes mecanismos*

Invariavelmente são necessárias informações e pressupostos com maior detalhe do que aqueles que estão disponíveis no imediato.

Em primeiro lugar, devem ser determinados os custos da implementação com rigor e precisão, uma vez que se tornará a base para a medição da eficácia em termos de custos. As perdas esperadas, caso não sejam tomadas acções, devem ser estimadas, para, através da comparação dos resultados, a gestão pode decidir se deve ou não implementar as medidas de controlo dos riscos.

O cumprimento de leis e regulamentações não é opcional. Uma organização deve entender as leis aplicáveis e implementar um sistema de controlo para estar em conformidade. Só pode haver alguma flexibilidade ocasional quando os custos da redução de um risco forem totalmente desproporcionais aos seus impactos.

Um dos métodos para a protecção financeira contra o impacto dos riscos é o financiamento através da contratação de seguros. Contudo, deve reconhecer-se que algumas perdas ou elementos de perdas podem não ser seguráveis, como por exemplo, certos custos relacionados com a saúde, segurança e incidentes ambientais, que englobem danos morais a empregados e à reputação da organização.



## 7. Comunicação de riscos

### 7.1. Comunicação interna

Dentro de uma organização os vários níveis necessitam de diferentes tipos de informações que serão obtidos através do processo de gestão de riscos.

**O Conselho de Administração deve:**

- *conhecer os riscos mais importantes que a organização enfrenta*
- *conhecer os possíveis efeitos no valor accionista provocados pelos desvios relativamente aos níveis de desempenho esperados*
- *garantir níveis adequados de sensibilização aos riscos em toda a organização*
- *saber de que forma a organização vai gerir uma crise*
- *conhecer o nível de confiança dos intervenientes na organização*
- *saber como gerir as comunicações com os investidores, quando aplicável*
- *ter a certeza de que o processo de gestão de riscos é eficaz*
- *publicar uma política de gestão de riscos clara que abranja a abordagem geral e as responsabilidades da gestão de riscos*

**As Unidades de Negócio devem:**

- *estar conscientes dos riscos inerentes às respectivas áreas de responsabilidade, dos possíveis impactos que estes podem ter noutras unidades e das consequências que outras unidades lhes podem provocar*
- *dispor de indicadores de desempenho que lhes permitam monitorizar nas actividades chave, quer financeiras quer operacionais, os progressos para o cumprimento dos objectivos*

- *identificar intervenções necessárias à correcção de desvios (por exemplo, previsões e orçamentos)*
- *dispor de sistemas que informem sobre variações orçamentais e de previsões, com uma frequência adequada, que permitam reacções apropriadas*
- *comunicar, sistemática e imediatamente, à direcção de topo todos os riscos novos ou falhas constatadas nas medidas de controlo existentes*

**Cada indivíduo deve:**

- *compreender o seu nível de responsabilização relativamente a riscos individuais*
- *compreender de que forma podem contribuir para a melhoria contínua da gestão de riscos*
- *compreender que a gestão de riscos e a sensibilização para a existência de riscos são elementos chave da cultura da organização*
- *comunicar, sistemática e imediatamente, à direcção de topo todos os riscos novos ou falhas constatadas nas medidas de controlo existentes*

### 7.2. Comunicação externa

Regularmente, uma empresa precisa de prestar contas aos intervenientes, definindo as respectivas políticas de gestão de riscos e a eficácia na obtenção de objectivos.

Cada vez mais, os intervenientes pretendem que as organizações apresentem provas de uma gestão eficaz do desempenho não financeiro, em áreas como assuntos da comunidade, direitos humanos, legislação laboral, saúde e segurança e meio ambiente.

**A boa gestão empresarial exige que as empresas adoptem uma abordagem metodológica para a gestão de riscos que:**



- *proteja os interesses dos intervenientes*
- *garanta que o Conselho de Administração cumpre os seus deveres relativamente à direcção da estratégia, construa valor e monitoriza o desempenho da organização*
- *garanta que os controlos de gestão estão implementados e funcionam correctamente*

As disposições relativas à comunicação formal da gestão de riscos devem ser claramente definidas e estar disponíveis para os intervenientes.

**A comunicação formal deve tratar de:**

- *métodos de controlo – em particular, responsabilidades de gestão relativas à gestão de riscos*
- *processos utilizados para identificar riscos e a forma como estes são tratados pelos sistemas de gestão*
- *principais sistemas de controlo implementados para gerir os riscos mais significativos*
- *sistema de monitorização e revisão implementado*

Todas as deficiências significativas não abrangidas pelo sistema, ou do próprio sistema, devem ser comunicadas em conjunto com os passos dados para corrigi-las.

## **8. Estrutura e administração da gestão de riscos**

### **8.1. Política de gestão de riscos**

Uma política de gestão de riscos deve definir a atitude e apetência para o risco e a abordagem para a gestão de riscos. A política deve também definir as responsabilidades relativas à gestão de riscos em toda a organização. Além disso, esta declaração de intenções deve também referir todos os requisitos legais aplicáveis, como por exemplo a nível de saúde e segurança.

Ligado ao processo de gestão de riscos está um conjunto de ferramentas e técnicas que deve ser utilizado nas várias etapas do processo de negócio.

**Para funcionar de forma eficaz, o processo de gestão de riscos exige:**

- *empenho por parte do Presidente e dos restantes membros do Conselho de Administração da organização*
- *a atribuição de responsabilidades dentro da organização*
- *a atribuição dos recursos adequados para a formação e o desenvolvimento de uma sensibilização ao risco de todos os intervenientes*

### **8.2. Papel do Conselho de Administração**

O Conselho de Administração tem a responsabilidade de definir a direcção estratégica da organização e criar o ambiente e as estruturas necessárias para que a gestão de riscos funcione de forma eficaz.

Estes deveres podem ser materializados através de um grupo executivo, de um comité não executivo, de um comité de auditoria ou de outra função que se adegue ao modo de funcionamento da organização e que seja capaz de actuar como ‘patrocinador’ da gestão de riscos.



O Conselho de Administração deve, quando avaliar o sistema de controlo interno, pelo menos, considerar:

- a natureza e extensão dos riscos de aspectos negativos aceitáveis para uma empresa, no contexto da sua actividade
- a probabilidade de esses riscos se tornarem uma realidade
- a forma como os riscos inaceitáveis devem ser geridos
- a capacidade da empresa minimizar a probabilidade e o impacto na actividade
- os custos e benefícios do risco e da actividade de controlo efectuada
- a eficácia do processo de gestão de riscos
- as implicações dos riscos nas decisões administrativas

### 8.3. Papel das unidades de negócio

Dentro das suas competências, estabelece o seguinte:

- as unidades de negócio têm a responsabilidade de gerir diariamente os riscos
- as direcções das unidades de negócio são responsáveis pela promoção da sensibilização sobre a existência de riscos nas respectivas actividades; devem introduzir objectivos de gestão de riscos nas suas unidades
- a gestão de riscos deve ser um tema regular das agendas das reuniões de direcção, de modo a permitir a consideração de exposições a riscos e a redefinição de prioridades das tarefas à luz de uma análise eficaz dos riscos
- as direcções das unidades de negócio devem garantir que a gestão de riscos é incorporada tanto na fase de concepção dos projectos, como ao longo da execução de cada um deles

### 8.4. Papel da Função gestão de riscos

Dependendo da dimensão da organização, o número de elementos envolvidos na gestão de riscos pode ir desde um único responsável até um departamento de grande escala.

A Função gestão de riscos deve incluir:

- a definição de políticas e estratégias de gestão de riscos
- o principal responsável pela gestão de riscos a nível estratégico e operacional
- o desenvolvimento da sensibilização para a existência de riscos dentro da organização, incluindo formação e informação adequadas
- o estabelecimento de políticas e estruturas de risco internas nas unidades de negócio
- a concepção e revisão de processos de gestão de riscos
- a coordenação de diversas actividades funcionais que forneçam aconselhamento sobre questões de gestão de riscos
- o desenvolvimento de processos de resposta a riscos, incluindo programas e/ou planos de contingência e de continuidade das actividades
- a preparação de relatórios sobre riscos para o Conselho de Administração e para os intervenientes

### 8.5. Função da auditoria interna

A função da auditoria interna será, com certeza, diferente em cada organização.

Na prática, a função da auditoria interna poderá incluir alguns ou todos os seguintes pontos:

- focar o trabalho da auditoria interna nos riscos significativos que foram identificados pela gestão da organização e fazer auditorias aos processos de gestão de riscos
- fornecer garantias sobre a gestão de riscos



- *proporcionar um apoio e um envolvimento activos ao processo de gestão de riscos*
- *possibilitar a identificação/avaliação de riscos e dar formação aos funcionários sobre gestão de riscos e controlo interno*
- *coordenar a comunicação de riscos ao Conselho de Administração, ao comité de auditoria, etc.*

Ao determinar a sua função mais adequada no contexto de uma determinada organização, a auditoria interna deve garantir que os requisitos profissionais de independência e objectividade não são postos em causa.

#### **8.6. Recursos e implementação**

Os recursos necessários para a implementação da política de gestão de riscos da organização devem ser claramente definidos para cada nível de gestão e dentro de cada unidade de negócio.

Para além de outras funções operacionais que possam ter, os elementos envolvidos na gestão de riscos devem ter as respectivas funções de coordenação de políticas/estratégias de gestão de riscos claramente definidas. Esta mesma definição é também necessária para os elementos envolvidos na auditoria e revisão de controlos internos e no facilitar do processo de gestão de riscos.

A gestão de riscos deve ser incorporada na organização através dos processos normais de definição de estratégias e orçamentos. Deve merecer destaque em todos os programas de indução, formação e desenvolvimento, assim como nos processos operacionais, como no caso dos projectos de desenvolvimento de produtos/serviços.

## **9. Monitorização e revisão do processo de gestão de riscos**

A gestão de riscos eficaz necessita de uma estrutura de comunicação e revisão que assegure que os riscos são identificados e avaliados de forma eficaz e que os controlos e respostas adequados são implementados. Devem ser executadas auditorias regulares ao cumprimento de políticas e normas e o desempenho, de acordo com as mesmas, deve ser revisto para identificar oportunidades de melhoria. É preciso não esquecer que as organizações são dinâmicas e funcionam em ambientes dinâmicos. As alterações à organização e ao ambiente no qual aquela funciona devem ser identificadas, para que sejam efectuadas as modificações adequadas aos sistemas.

O processo de monitorização deve garantir que estão implementados os controlos adequados para as actividades da organização e que os procedimentos são compreendidos e seguidos. As alterações à organização e ao ambiente no qual se insere devem ser identificadas, para que sejam efectuadas as mudanças adequadas aos sistemas.

#### **Qualquer processo de monitorização e revisão deve determinar se:**

- *as medidas adoptadas alcançaram os resultados pretendidos*
- *os procedimentos adoptados e as informações recolhidas para a realização da avaliação foram os adequados*
- *um melhor nível de conhecimento teria ajudado a tomar melhores decisões e a identificar a possibilidade de tirar ilações para futuras avaliações.*



## 10. Anexos

### Técnicas de identificação de riscos exemplos

- *Brainstorming*
- *Questionários*
- *Estudos que analisem cada processo da actividade e descrevam os factores internos e externos que possam influenciar os referidos processos*
- *Análises comparativas do sector*
- *Análises de cenários*
- *Oficinas de avaliação de riscos (workshops)*
- *Investigação de incidentes*
- *Auditorias e inspecções*
- *HAZOP (Hazard & Operability Studies)*

### Métodos e técnicas de análise de riscos exemplos

#### Riscos de aspectos positivos

- *Estudos de mercado*
- *Prospecções*
- *Testes de marketing*
- *Investigação & Desenvolvimento*
- *Análises do impacto sobre a actividade*

#### Ambos

- *Modelos de dependência*
- *Análises SWOT (Pontos fortes, Pontos fracos, Oportunidades, Ameaças)*
- *Árvore/Análises de eventos*
- *Planos de Contingência e Continuidade do Negócio*
- *Análises NPEST (Negócio, Política, Económica, Social, Tecnológica)*
- *Modelos de opções reais*
- *Tomadas de decisões em condições de risco e incerteza*
- *Inferências estatísticas*
- *Medições de tendência central e dispersão*
- *PESTLE (Políticos, Económicos, Sociais, Técnicos, Legais, Ambientais)*

#### Riscos de aspectos negativos

- *Análises de ameaças*
- *Árvore de falhas*
- *FMEA (Failure Mode and Effect Analyses)*

*As páginas seguintes contêm excertos do documento PD ISO/IEC Guide 73: 2002 reproduzidos por autorização do British Standards Institution ao abrigo da licença com o número*

*2002SK/0313. As Normas Britânicas podem ser obtidas através do Customer Services (Serviço ao Cliente) da BSI,*

*389 Chiswick High Road, London W4 4AL. (Tel + 44 (0) 20 8996 9001*



**AGERS** - Asociación Española de Gerencia de Riesgos y Seguros  
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.- 28006 Madrid - SPAIN  
Tel: + 34 91 562 84 25 – Fax: + 34 91 590 07 80 – Email: gerencia@agers.es – www.agers.es



**AIRMIC** - The association of Insurance and Risk Managers  
Lloyd's Avenue, 6 – London EC3N3AX - UK  
Tel: + 44 207 480 76 10 – Fax: + 44 207 702 37 52 – Email: enquiries@airmic.co.uk – www.airmic.com



**AMRAE** - Association pour le Management des Risques et des Assurances de l'Entreprise  
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE  
Tel: + 33 1 42 89 33 16 – Fax: + 33 1 42 89 33 14 – Email: amrae@amrae.fr – www.amrae.fr



**ANRA** - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali  
Via del Gonfalone 3, I-20123 Milano - ITALY  
Tel: + 39 02 58 10 33 00 – Fax: + 39 02 58 10 32 33 – Email: anra@betam.it – www.anra.it



**APOGERIS** - Associação Portuguesa de Gestão de Riscos e Seguros  
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – PORTUGAL  
Tel: + 351 22 608 24 62 – Fax: + 351 22 608 24 73 – E-mail: anfernandes@sonae.pt – www.apogeris.pt



**ASPAR CR** - Association of Insurance and Risk Management of the Czech Republic o.s.  
Nad Ohradou 7 – 13000 Praha 3 – Tel: + 420 602 384 256 – Email: asparcr@volny.cz



**BELRIM** - Belgian Risk Management Association  
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM  
Tel: + 32 2 389 23 95 – Fax: + 32 2 389 22 72 – Email: info@belrim.com – www.belrim.com



**bfv** - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften e.V.  
c/o Mr Hans-Otto GEIGER – Postfach 1916 – D-67209 Frankenthal – GERMANY  
Tel: + 49 6233 86 2507 - Fax: + 49 6233 86 2507 - Email: hans-otto.geiger@ksb.com – www.bfv-fvv.de



**BRIMA** - Bulgarian Risk Management Association  
101, Tzarigradsko chaussee, floor 4 – Sofia 1113 – BULGARIA  
Tel: + 359 878 100292 – Fax: + 359 2 971 0702 – Email: office@brima.biz – www.brima.biz



**DARIM** - DI's Risk Management Forening  
DK-1787 Copenhagen – DENMARK  
Tel: + 45 33 77 33 77 – Fax: + 45 33 77 33 00 – Email: darim@di.dk – www.di.dk



**DVS** - Deutscher Versicherungs-Schutzverband e.V.  
Breite Strasse 98 - D 53111 Bonn - GERMANY  
Tel: + 49 228 98 22 30 - Fax: + 49 228 63 16 51- Email: dvs@dvs-schutzverband.de – www.dvs-schutzverband.de



**FINNRIMA** - Finnish Risk Management Association  
Talvikkitie 40 A 33, 01300 Vantaa – FINLAND  
Tel: + 358 9 5607 5361 – Fax: + 358 9 5607 5365 – Email: srhy@hennax.fi – www.srhy.fi



**NARIM** - Nederlandse Associatie van Risk en Insurance Managers  
P.O. Box 65707 - 2506 EA Den Haag – THE NETHERLANDS  
Tel: + 31 70 345 7426 – Fax: + 31 70 427 3263 – Email: ielsdewild@imfo.nl – www.narim.com



**POLRISK** - Polish Risk Management Association  
ul. Rzymowskiego 30 lok. 424 - 02-697 Warszawa - POLAND  
Tel: + 48 22 331 8121 – Fax: + 48 22 331 81 22 – Email: info@polrisk.pl – www.polrisk.pl



**RUSRISK** - Russian Risk Management Society  
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070 – RUSSIA  
Tel: + 7 495 231 53 56 - Fax: + 7 495 231 53 56 - Email: info@rrms.ru – www.rrms.ru



**SIRM** - Swiss Association of Insurance and Risk Managers  
Gutenbergstrasse 1, Postfach 5464, CH-3001 Bern - SWITZERLAND  
Tel: + 41 31 388 87 89 – Fax: + 41 31 388 87 88 – Email: info@sirm.ch – www.sirm.ch

**SWERMA** - Swedish Risk Management Association  
Gränsvägen 15 - SE-135 47 Tyresö - SWEDEN  
Tel: + 468 742 13 07 - Fax: + 468 798 83 11- E-mail: info@swerma.se – www.swerma.se

**ALARM** - The National Forum for Risk Management in the Public Sector  
Queens Drive, Exmouth - Devon, EX8 2AY  
Tel: + 44 1395 223399 - Fax: + 44 1395 223304 - Email: admin@alarm.uk.com - www.alarm-uk.com



**IRM** - The Institute of Risk Management  
6 Lloyd's Avenue - London EC3N 3AX  
Tel: + 44 20 7709 9808 - Facsimile + 44 20 7709 0716 - Email: enquiries@theirm.org - www.theirm.org