

**ACIDENTES NAS PLATAFORMAS:  
por que a GR não evita**

**ENTREVISTA**

**31010 por Antonio Brasiliano**

**GRTI**

**O novo risco de quem para**



**apetite ao risco: TECNICIDADE X OUSADIA**

**sua EMPRESA está PREPARADA?**



informações | [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)



## Editorial

### Em Foco

Gestão de Riscos em plataformas marítimas .....07

Gestão de Riscos e a ISO 31000 .....10

### Entrevista

31010 Técnicas de avaliação de riscos.....14

### Análise

O papel da area de Gestão de Riscos nas empresas .....26

### Acontece

#### GRTI

Uma nova categoria de risco: a inércia .....37

### Carreira

Gerenciando o superior hierárquico .....41

### Ler&Saber

A revista Gestão de Riscos é uma publicação eletrônica mensal da Sicurezza Editora.

Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL

**Diretores** | Antonio Celso Ribeiro Brasileiro e Enza Cirelli. **Edição e Revisão** | Mariana Fernandez. **Arte e Diagramação** | Agencia BM Design

**Colunista** | Mariana Fernandez **Colaboradores desta edição** | Andre Pitkowski, Nino Ricardo Meireles, Renato Vial Polidori, Rosangela Aparecida Stringuer

**Brasiliano & Associados Online** | [www.brasiliano.com.br](http://www.brasiliano.com.br) **Blog da Brasiliano & Associados** | [www.brasiliano.com.br/blog](http://www.brasiliano.com.br/blog)

## ABAIXO A MIOPIA

O artigo especial deste mês que trata da Gestão de Riscos nas plataformas marítimas é uma verdadeira lente para que você leitor possa enxergar os equívocos provocados pela miopia organizacional que engloba, inclusive, a gestão dos riscos corporativos. Desde o acidente com a plataforma Deepwater Horizon, no último dia 20 de abril, o custo/ benefício da extração de combustíveis fósseis voltou a ser questionada, perante o desastre causado ao ecossistema do Oceano Atlântico onde medidas emergenciais de contingência só conseguem recuperar de 10% a 15% do óleo cru derramado. Outra questão levantada a partir do acidente foi a da possibilidade de ocorrer algo parecido em águas brasileiras uma vez que o problema se deu devido a uma falha num equipamento que é usado em todas as perfurações marítimas em águas profundas.

Mas num ângulo mais amplo abordamos a GR nas plataformas, listando e analisando os diversificados acidentes que ocorrem sobre as Unidades Marítimas de Produção em território brasileiro e internacional. A negligência para com os incidentes periódicos se mostra como a maior causa para os acidentes que atentam contra a vida dos homens, das empresas e do meio ambiente.

Já em outra seção e para auxiliar na eficiência dos controles, Antonio Celso Ribeiro Brasileiro dá a sua contribuição através de uma entrevista focada nas técnicas e ferramentas de gestão de riscos contempladas na norma ISO 31010. Brasileiro é o brasileiro criador do método de Gestão e Análise de Riscos que constará na próxima revisão da norma internacional.

Para não fazer você perder o fio da meada, Rosângela Aparecida Stringuer retoma a norma ISO 31000, esclarecendo a função da normativa e o objetivo da área de GR e, num panorama mais amplo, Renato Vial Polidori se aprofunda no papel da área nas empresas.

Nino Ricardo Meireles também combate a miopia nesta edição, ensinando como gerenciar o superior hierárquico através de uma conscientização do relacionamento do gestor com seu “chefe” na organização.

Na coluna deste mês, Andre Pitkowski, também focaliza um tema mal percebido, deixando nítidas as vantagens da busca constante pela agilidade, mostrando a inércia como uma nova categoria de risco.

Bons olhos para uma boa leitura,

Mariana Fernandez  
Editora

# Serviços de Consultoria

## Plano de Continuidade de Negócios - PCN

### Sua empresa está preparada para um evento de DESCONTINUIDADE??

A operacionalização de um PCN é um processo estruturado para:

- Melhorar proativamente a resiliência da empresa contra possíveis descontinuidade;
- Restabelecer a capacidade de fornecimento de produtos e serviços;
- Proteger marca e reputação

O PCN possui normatizações e regulações, com base nas melhores práticas internacionais.

No Brasil, através da ABNT, tem as normas ABNT NBR 15999 - 1 e 2, que descrevem o processo, estrutura e conteúdo de um sistema de Gestão de Continuidade de Negócio.

## Capacite sua empresa para resistir aos efeitos de um incidente!!!!

## Consulte – nos!!!!

informações | 11 5531-6171  
| [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)







# Acidentes Ambientais nas Plataformas: cadê a GR?

*Mariana Fernandez*

## **INCIDENTES INCONTROLADOS, ACIDENTES FATAIS**

Acidentes dos mais variados tipos já se tornaram comuns em plataformas de extração de petróleo, desde os que provocam imensos danos ambientais e financeiros, até os que roubam um punhado de vidas de cada vez.

Segundo o presidente da Sociedade Brasileira de Engenharia de Segurança, Reynaldo Barros, quando do acidente com a plataforma P-36 da Petrobrás (vide texto nas páginas seguintes), “para cada acidente grave, existem dez de menor relevância”. Ou seja, controles mais rigorosos podem ajudar a evitar desastres e mais ainda, o erro das administradoras das plataformas está em não tirar de seus incidentes as lições necessárias para evitar uma grande tragédia.

O trabalho Análise de causas de acidentes de trabalho nas plataformas de petróleo na Bacia de Campos, desenvolvido no Centro de Estudos da Saúde do Trabalhador e Ecologia Humana na Escola Nacional de Saúde Pública da Fundação Oswaldo Cruz refere-se, igualmente, à negligência dos incidentes no prejuízo da prevenção de acidentes nas unidades marítimas de produção. Segundo ele, uma falha crucial encontra-se na “subestimação, manifestada através



do sub-registro dos mesmos (incidentes), já que constituem apenas um quinto do total de acidentes quando deveria no mínimo ser o contrário, deixa de ser apenas um problema de registro, mas também, e principalmente um problema de segurança, pois as falhas latentes que podem estar se ocultando em determinado momento podem, no momento seguinte, se transformar em acidentes que ameaçam a saúde e a vida dos trabalhadores”.

## TRAGÉDIAS RECENTES

O último acidente noticiado ocorrido numa plataforma petrolífera ocorreu no último dia 17 de maio, deixando dois mortos e dois feridos. A ocorrência deu-se

na sonda de perfuração Ocean Ambassador, afretada à OGX, instalada na na Bacia de Campos, norte fluminense. Os quatro tripulantes vitimados faziam um teste de rotina na baleeira (barco de emergência), quando a embarcação caiu no mar, durante a operação em que era retirada da água.

A Capitania dos Portos do Rio abriu um Inquérito Administrativo sobre Acidentes e Fatos da Navegação para apurar as causas e circunstâncias do acidente. O relatório será enviado para julgamento do Tribunal Marítimo. A previsão de conclusão é de 90 dias.

Em abril, a tragédia espalhou-se pelas correntes marítimas do Atlântico, com a explosão da plataforma Deepwater Horizon no Golfo do México. (Veja quadro abaixo).

## ATAQUE AO ATLÂNTICO

Um gravíssimo acidente atingiu o Oceano Atlântico no primeiro semestre deste ano. A explosão da plataforma Deepwater Horizon, no dia 20 de abril, reabre a discussão sobre os perigos e impactos da extração de petróleo. O acidente ocorrido no Golfo do México deixa em alerta governos e pesquisadores de todo o mundo, inclusive no Brasil, grande explorador de petróleo no mar.

A plataforma petrolífera semi submersível, que pertence à Transocean e que estava sendo operada pela British Petroleum (BP) pegou fogo no dia 21 de abril. A explosão ocorreu na madrugada de terça para quarta-feira, 21 de abril, em frente à costa do estado americano da Louisiana, a cerca de 75 km da cidade de Venice. Depois de ficar dois dias em chamas, afundou, a 80 quilômetros da costa do estado americano da Louisiana. Dezesete trabalhadores estão feridos e onze desaparecidos.

A fratura na tubulação que era conectada à plataforma a partir da cabeça do poço, a mais de uma milha da superfície, segue lançando cerca de cinco mil barris, ou 800 mil litros, de petróleo por dia no mar, causando um dos maiores desastres ambientais da história da indústria petroleira.

A plataforma realizava perfurações exploratórias 84 quilômetros ao sudoeste de Venice, na Louisiana, quando ocorreu a explosão.

Plataformas como a Deepwater Horizon não são ancoradas no fundo do mar, são flutuantes, o que permite que trabalhem em profundezas de água de até 3.000 metros. Plata-

formas deste tipo usam um complicado sistema de posicionamento, que inclui motores e GPS, para mantê-las sempre na mesma posição.

O acidente foi desencadeado por uma bolha de metano que escapou do poço e disparou para cima, pela coluna de perfuração, expandindo-se rapidamente ao eclodir através de diversos lacres e barreiras antes de explodir, informaram funcionários da plataforma entrevistados pela BP, que conduz uma investigação interna do caso.

No ano passado, a BP foi multada em US\$ 87 milhões por não ter melhorado as condições de segurança depois de uma enorme explosão que provocou a morte de 15 pessoas em uma refinaria na cidade do Texas.

O Serviço de Administração Mineral dos Estados Unidos tinha realizado inspeções de rotina na plataforma Deepwater Horizon em fevereiro, março e abril deste ano, sem encontrar nenhuma violação às normas de segurança.

*Imagem de satélite divulgada no último dia 17 de maio pela Nasa mostra o avanço da mancha de óleo. (Foto: AP)*



## **Aposentado**

Chris Oynes, diretor responsável pelo setor de controle da exploração de energia no mar do Serviço de Gerenciamento de Minerais dos Estados Unidos (MMS, da sigla em inglês) - agência federal acusada de ter sido leniente com as petroleiras, abrindo caminho para o desastre do Golfo do México - anunciou sua aposentadoria nesta segunda-feira, informou o órgão.

Oynes foi nomeado em 2007 diretor associado do programa de exploração de energia mineral no mar do MMS, com responsabilidades que incluíam controlar os programas de exploração de petróleo e gás fora do continente.

A decisão ocorre em um momento em que a agência é criticada por ter sido muito leniente com as empresas petroleiras em suas inspeções da exploração de petróleo no mar, e de ser muito próxima das companhias as quais é encarregada de fiscalizar.

## **Riscos Ambientais**

A emissão de petróleo no mar coloca em risco a vida marinha em uma região de terras baixas que contém zonas vitais de desova para peixes, camarões e caranguejos, além



de consistirem em parada importante para muitas espécies migratórias de aves raras, afirmam especialistas.

Os danos aos ecossistemas marinhos, caso isso ocorra, serão “incalculáveis”, disse o professor da Faculdade de Ciências Marinhas da Universidade de Miami Daniel Suman, à EFE. No local vivem animais ameaçados de extinção, como o jacaré americano, pelicano marrom, tubarão azul, baleias e tartarugas. Na quinta-feira, 6 de maio, uma reserva ecológica de Luisiana foi atingida pela mancha.

O óleo ainda pode destruir a vegetação que serve de alimento para os peixes – a base da cadeia alimentar, alertam os estudiosos. Com isso, a atividade de criadores de camarões e pescadores está em risco. Só a pesca local movimentava mais de 40 bilhões de dólares por ano. A atividade foi banida enquanto a situação não é resolvida e cerca de 4,5% da área do Golfo está proibida para os pescadores.

### **Medidas de retenção**

Inúmeras ações, todas fracassadas até o momento, já foram tomadas pelas BP para tentar conter o vazamento de petróleo. A lâmina d'água de trabalho (1.500 metros) e a profundidade do poço (5.400 metros) tornam o desafio da empresa ainda maior.



*Animais marinhos mortos já começam a ser encontrados nas praias da região/Foto: Joe Raedle*



*Barcos tentam conter a mancha de petróleo com barreiras flutuantes/ Foto: US Coast Guard*

Em Washington, considerações de segurança ambiental já fizeram o presidente Obama recuar da decisão de permitir perfurações no mar e condicioná-las à segurança. O presidente afirmou ainda que quer endurecer a legislação sobre compensações por danos em caso de vazamentos de petróleo, que atualmente limita esses pagamentos a US\$ 75 milhões.

Mesmo com tudo isso, o analista ambiental do IBAMA Cristiano Vilardo é cético quanto aos resultados das ações. “Em condições ótimas, tempo bom, resposta rápida, equipamentos modernos, uma ação de contingência consegue recuperar de 10% a 15% do óleo cru derramado no oceano. Se algum fator complicador estiver presente, como ventos, correntes ou ondas, esse percentual é reduzido consideravelmente”, explicou.

*Até cabelo humano e pelo de animais têm sido usados para tentar conter a mancha/Foto: Matter of Trust*



### **Riscos para o Brasil**

“Um incidente com as mesmas características deste que ocorre nos EUA é passível de ocorrer no Brasil, uma vez que o problema se deu devido a uma falha num equipamento que é usado em todas as perfurações marítimas em águas profundas”, alertou o analista ambiental da HidroClean Proteção Ambiental, Maurício Green, e o seu diretor Carlos Boeckh, que também é coordenador do Plano de Emergência da Baía de Guanabara (PEBG).

Já Cristiano Vilardo alerta que, apesar de existirem simulados de emergência onde são testados os procedimentos de comunicação, mobilização de recursos e efetividade da resposta aos derramamentos de óleo, e da tentativa de aprovação de um Plano Nacional de Contingência, as empresas “estão passando de raspão nesses exames”.

“São raros os exercícios de simulação onde não se tenha problemas com o lançamento de barreiras, ou falhas de comunicação, ou defeito em embarcações, ou todas as alternativas anteriores. Nesses casos, o IBAMA tem atuado exigindo a correção dos erros e, eventualmente, a realização de novo exercício completo”, diz.

O analista afirma que a situação fica ainda mais crítica quando são avaliados blocos situados muito próximos de áreas ambientalmente relevantes. “Podemos citar, por exemplo, a existência de blocos petrolíferos a menos de 10 km do litoral paradisíaco do baixo sul da Bahia, ainda em licenciamento ambiental. Nesses casos, se um vazamento de óleo ‘acontecer’, não há plano de emergência que dê conta de evitar uma tragédia ambiental”, diz.

Os reflexos do vazamento no Golfo do México levaram o Governo do Estado do Rio e o Ministério do Meio Ambiente a formar um grupo de trabalho, que fará a prevenção e o mapeamento dos eventuais riscos em plataformas de petróleo no Brasil. A reunião foi realizada no dia 7 de maio, na sede da Secretaria do Ambiente do Estado do Rio.

*800 mil litros de petróleo são despejados no mar diariamente  
Foto: US Coast Guard*



### **Avaliação do desastre**

Para o cientista político Sérgio Abranches, não existe tecnologia adequada para lidar com esse tipo de vazamento. “O desastre ocorre na maior e mais rica economia do mundo, no país mais avançando tecnologicamente e em um projeto de uma grande e avançada empresa. Ela pediu ajuda a suas concorrentes e as poucas sugestões que recebeu foram típicas. Ninguém sabe como estancar o vazamento naquela profundidade em tempo de evitar um desastre dessas proporções”.

Abranches sugere quatro grandes lições a serem extraídas do episódio: “A primeira é que o risco é maior do que as empresas admitem. A segunda é que não existe tecnologia adequada nem para prevenção desse risco, nem para controlar prontamente os danos, menos ainda para estancar o processo em tempo hábil. A terceira é que esses desastres têm consequências de longo prazo. A quarta lição é que esses projetos petrolíferos em águas profundas têm um custo escondido”, opina.





Há analistas como Jeff Rubin que comparam este acidente com o acidente de Chernobyl, sugerindo uma possível estagnação nessa modalidade de exploração como teria ocorrido com a energia nuclear.

### **Possíveis Causas do Acidente**

Ainda não há conclusão sobre a causa do acidente com a plataforma. As investigações sobre a causa estão centradas basicamente em duas hipóteses: i) problemas no processo de cimentação e; ii) falha do Blowout Preventer (BOP). Inúmeros problemas incomuns foram identificados no BOP, o que torna o caso permeado de mistério, deixando margem para especulações de diversas naturezas. Segundo inquérito interno da BP a explosão ocorreu porque a tampa do poço teria falhado devido a uma bolha de metano que escapou do poço, foi lançada pela coluna de perfuração e se expandiu rapidamente, porque rompeu várias barreiras de segurança e lacres de cimento até explodir. Tudo isso teria ocorrido ao longo da cimentação. De fato a fase de cimentação envolve um elevado risco de blowout. De acordo com um estudo de 2007 da Minerals Management Service, o cimento foi um fator relevante em 18 das 39 rupturas em plataforma ocorridas no Golfo do México, entre 1992 e 2006.

Esse acidente alerta para o fato de que os procedimentos de segurança podem falhar, incluindo o BOP (blowout preventer). Trata-se de um sistema de segurança na saída para o solo oceânico. Por causa do acidente, o tubo que liga o poço à plataforma foi danificado sendo impossível acessá-lo. Os BOPs constituem a mais moderna resposta da indústria para o blowout e não haviam falhado desta forma antes. O evento aumenta as exigências de segurança e tendem a reduzir a probabilidade de algo semelhante se repetir. A BP alertou que ocorreu um número inédito de falhas e muitos detalhes ainda não foram esclarecidos. Há também relatos de possíveis problemas na própria construção da plataforma Deepwater Horizon, no ano de 2001, nos estaleiros coreanos da Hyundai. Este tipo de plataforma semi-submersível utiliza um sistema de geo-posicionamento dinâmico que lhe permite permanecer fixa em relação a um ponto no fundo do mar. São utilizados sensores de correntes e ventos para ativar os motores e mantê-la fixa. Esta tecnologia corresponde ao que tem de mais moderno no segmento *offshore* da indústria.

No dia 29 de maio o New York Times divulgou que há um ano a BP tinha informações quanto aos riscos naquela plataforma. No dia 22 de junho de 2009, em documentos internos à companhia, um engenheiro de perfuração sênior chamado Mark E. Hafle alertou que o revestimento de metal que a empresa queria usar no poço poderia sofrer um colapso sob altas pressões. No entanto, ele relativizou afirmando que a ocorrência do problema estaria associada a um cenário pessimista – raro, mas possível. Depois de outros acidentes envolvendo a empresa, especialmente desde 2007, a BP vinha tentando reverter sua política (ineficiente) de cortes de custos, a qual também estava sendo associada aos incidentes ocorridos.

Ademais, segundo memorando dos representantes da Comissão de Energia e Comércio dos EUA que investiga o caso, antes da explosão os operadores da plataforma receberam três alarmes sobre problemas de fluxo no poço. A BP teria informado que o primeiro alarme teria ocorrido 51 minutos antes da explosão, quando o fluxo superou o padrão de bombeamento. O segundo aviso teria ocorrido aos 41 minutos antes da explosão,

quando houve um inesperado aumento de pressão. O último alerta veio 18 minutos antes da explosão, “diante de pressões anormais e da presença de lodo, quando o bombeamento foi interrompido abruptamente”. Também há indícios de que os operários da plataforma tentaram controlar a pressão antes da explosão. Imagens oferecidas pela BP mostram como o petróleo estava saindo pelas quatro válvulas da estrutura instalada. De acordo com o memorando os dados sugerem que a tripulação pode ter tentado intervenções mecânicas nesse ponto para controlar a pressão, mas logo depois, o fluxo saiu do controle, a pressão aumentou dramaticamente e ocorreu a explosão. Mesmo diante das informações que vão surgindo ao longo das investigações ainda não foi possível identificar a causa que está na raiz do acidente.

## **AS LIÇÕES DO DESASTRE DA DEEPWATER HORIZON**

*Por Priscila De Martini*

O que é preciso fazer no Brasil, segundo especialistas:

### **Aumentar multas**

A legislação brasileira prevê multa de R\$ 7 mil a R\$ 50 milhões para as empresas do setor petrolífero responsáveis por acidentes em águas sob jurisdição nacional (excluídos os custos com limpeza e possíveis indenizações). O diretor-geral da Agência Nacional do Petróleo (ANP), Haroldo Lima, porém, afirmou que o valor-limite de R\$ 50 milhões tornou-se muito baixo diante do acidente ocorrido no Golfo do México. Especialistas também alegam que a legislação não é clara o suficiente na definição dos critérios para a aplicação das penalidades.

### **Plano emergencial**

Deveria ser criado o Plano Nacional de Contingência para Derramamento de Óleo (PNC), inexistente mesmo depois de ter sido exigido pela legislação há 10 anos. Atualmente, os planos de emergência são individuais (para cada plataforma, por exemplo). Já o PNC é um documento nacional, que consolida todas as atribuições de empresas e governos no caso de um acidente, sobretudo em episódios mais graves.

### **Menos poder à Petrobras**

Para Doneivan Ferreira, especialista em economia do petróleo, a Petrobras deveria ter menos influência no governo: Se a companhia é tão forte e tem tanto poder que o órgão regulador não consegue fazer exatamente o que ele quer, manter essa empresa na linha, até em termos de segurança, pode se tornar um risco. É muito importante que o Brasil se desenvolva, e os recursos do pré-sal são importantes no momento. Agora, tem que saber se o poder dado à Petrobras não vai fazer dela uma empresa intocável. Ela tem que ser uma empresa regulável.



## Corpo técnico

Ferreira alerta que o Ibama não tem um corpo técnico adequado para avaliar o licenciamento para exploração de petróleo. Além disso, a burocracia dos órgãos reguladores seria um entrave: “A ANP licenciou algumas áreas que estão dentro de uma zona em que o Ibama não dá licença. Isso é culpa da agência de não ter visto isso antes.”

## ACIDENTES “PETROBRASILEIROS”

No ano passado, um acidente na plataforma P-34 da Petrobras, no litoral sul do Espírito Santo, resultou na morte de um caldeireiro na noite do dia 4 de janeiro de 2009. Segundo o Sindicato dos Petroleiros do estado, por volta 23h15 de domingo houve uma falha em uma válvula de bloqueio da plataforma, o que provocou o vazamento de água e óleo. O material teria escapado com muita pressão e atingiu William Robson Vasconcelos, de 28 anos. Outros dois funcionários tiveram escoriações leves. A Petrobras informou ter instaurado uma comissão técnica para avaliar as causas do acidente.

Em 2008, um funcionário terceirizado da Petrobras morreu em consequência de um acidente na tarde do dia 11 de junho, durante a operação da plataforma de perfuração SS-49. A Petrobras abriu sindicância para apurar as causas do acidente.

Em 3 de março de 2002, um acidente na plataforma P-15 da Petrobras, provocado por um vazamento de ar comprimido, apavorou os funcionários, que foram transferidos para outras plataformas. Uma tubulação de ar formou várias bolhas no mar da Bacia de Campos, onde se localizava a plataforma. As atividades voltaram ao normal no dia seguinte ao acidente.

No mesmo dia, outro acidente, um mergulhador morreu na plataforma 20, em seu primeiro dia de trabalho. Marcos Francisco da Silva era funcionário de uma prestadora de serviços da Petrobrás.

2001 foi o ano da superação. Com três explosões e dez mortes, a plataforma P-36 da não manchou apenas a Bacia de Campos mas a imagem da Petrobras e do Brasil. (Vide quadro ao lado)

Nos quinze meses que se antecederam à catástrofe, a empresa viu-se envolvida em 95 acidentes, nos quais morreram dezoito pessoas. Como se não bastasse, no período de 2000 a 2001, seus dutos foram responsáveis por quatro vazamentos gigantes, que despejaram 5,5 milhões de litros de óleo por lagoas, rios e baías.

Em 2000, três plataformas da Petrobrás tiveram incêndios debelados. (Veja quadro com os maiores acidentes da história da Petrobras).

### P-36: O GRANDE DESASTRE BRASILEIRO

Em 20 de março de 2001, ocorreu o maior acidente brasileiro em plataformas petrolíferas na instalação responsável pela extração de 6% do petróleo brasileiro.

## IMAGEM MARCADA

Alguns dos maiores acidentes da história da Petrobras

**Morretes, Paraná, em fevereiro de 2001:**

O rompimento de um oleoduto provocou o vazamento de 50.000 litros de óleo diesel, que atingiram rios da região

**Baía de Guanabara, Rio de Janeiro, em janeiro de 2000:**

Vazamento na Refinaria Duque de Caixias espalhou 1,3 milhão de litros de óleo por mais de 50 quilômetros quadrados

**São Sebastião, São Paulo, em janeiro de 1992:**

Um navio explodiu depois de descarregar óleo no terminal da Petrobras. Uma pessoa morreu

**Bacia de Campos, Rio de Janeiro, em agosto de 1984:**

Vazamento de gás provoca incêndio na plataforma de Enchova. Houve 37 mortes

**Cubatão, São Paulo, em 1984:**

Um vazamento incendeia uma vila vizinha aos dutos da Petrobras, noventa pessoas morreram





Às 2 e meia da madrugada, a monumental construção, equivalente a um prédio de quarenta andares e à largura de um quarteirão, começou a adernar, a 120 km da costa do Rio de Janeiro. A P-36, que custou ao país 430 milhões de dólares, estava operando havia um ano no campo de Roncador, uma das áreas mais promissoras de produção da Bacia de Campos, de onde saem 90% do petróleo brasileiro.

A vitória já vinha sendo comemorada pelo governo. Desde que a plataforma começou a operar no campo de Roncador, em março do ano passado, o Brasil economizou em média 2 milhões de dólares ao dia em importação de petróleo.

No dia seguinte ao desastre, já era possível fazer um cálculo preliminar do estrago. A estimativa é de que o país tenha um prejuízo de mais de 1 bilhão de dólares ao ano. Os analistas avaliam que a perda resultante da interrupção da produção de 80.000 barris de petróleo seja em torno de 600 milhões de dólares ao ano.

Uma plataforma como a P-36, mesmo sem afundar, leva quase esse tempo para ser consertada. A construção de uma plataforma igual tomaria no mínimo três anos.

Foi o pior acidente em plataforma de petróleo no país desde 1984, quando uma explosão na plataforma de Enchova, também na Bacia de Campos, deixou o trágico saldo de 37 mortos.

## Perdas Financeiras

Apesar de o seguro da plataforma ser avaliado em 500 milhões de dólares, não há contrato que cubra o prejuízo com a paralisação da produção. Para o país, porém a perda é mais estrondosa ainda. Logo que foram anunciados o acidente e a extensão do estrago, as ações da companhia nas bolsas de valores despencaram no Brasil e em Nova York. O dólar, que já vinha pressionado pela crise argentina e pelo temor de recessão nas principais economias do mundo, teve uma nova alta. Isso obrigou o Banco Central a intervir. Vendeu dólares de suas reservas, para tentar conter a subida. Além disso, perder produção num momento em que os preços do petróleo voltam a subir no mercado internacional é um prejuízo que o país não podia dar-se ao luxo de sofrer.

## Cadê a segurança?

O acidente na P-36 também chamou a atenção para uma questão que vem sendo insistentemente discutida pelos funcionários, depois de tantos acidentes: a segurança. Na briga entrou até o Ministério Público do Trabalho, que acusa a Petrobras de negligenciar o controle da contratação de mão-de-obra terceirizada. Desde 1995, a companhia iniciou um processo de incentivo a aposentadorias e demissões, passando a contratar mão-de-obra terceirizada para várias funções. O presidente da Associação dos Engenheiros da Petrobras, Fernando Siqueira, aponta como o maior problema a baixa qualificação das empreiteiras que trabalham com a companhia. "Nos Estados Unidos, eles trabalham com terceirizados de empresas de ponta. Aqui, a contratação é aberta



para qualquer empresinha de fundo de quintal”, protesta. A própria Petrobras reconhece que precisa dar melhor treinamento ao pessoal terceirizado. E a Agência Nacional de Petróleo (ANP), uma semana antes do acidente com a P-36, já tinha dado um puxão de orelhas na empresa nesse sentido. Mas no caso específico da explosão na Bacia de Campos não há indícios de que problemas de treinamento de terceirizados tenham provocado a tragédia.

### **Causa provável**

O engenheiro Segen Estefen, diretor da Coordenação dos Programas de Pós-Graduação em Engenharia (Coppe), da Universidade Federal do Rio de Janeiro, levanta a hipótese de erro no projeto da plataforma. A P-36 foi encomendada na gestão de Joel Rennó, que comandou a Petrobras entre 1992 e 1999, e sempre esteve envolta em polêmica e acusações de favorecimento. O empresário que ganhou a licitação contratou a obra num estaleiro italiano que faliu. O projeto foi transferido para o Canadá e modificado por outro estaleiro. Desde 1980, quando uma plataforma da Noruega afundou no Mar do Norte, as plataformas têm de obedecer a especificações para evitar que explosões resultem em afundamento. Suspeita-se que a P-36 não esteja dentro dessas normas. Só as investigações vão dizer o que realmente aconteceu na madrugada do acidente. Por isso, a Petrobras recusa-se a se manifestar sobre possíveis causas da tragédia.

## **O ACIDENTE**

**0h20** Um vazamento de gás na coluna de sustentação provoca uma explosão seguida de incêndio. A primeira brigada de incêndio é acionada.

**0h50** A brigada é surpreendida por uma segunda explosão. Os cinco integrantes morrem. A segunda brigada entra em ação. Uma terceira explosão acontece em seguida e mata os outros cinco encarregados de debelar o fogo.

Uma brigada de socorristas é acionada. Resgata o corpo de um dos membros da brigada de incêndio e retira do local do acidente o operador Sergio Santos Barbosa. Um helicóptero-ambulância leva Barbosa para o hospital da Base Aérea do Galeão, no Rio de Janeiro.

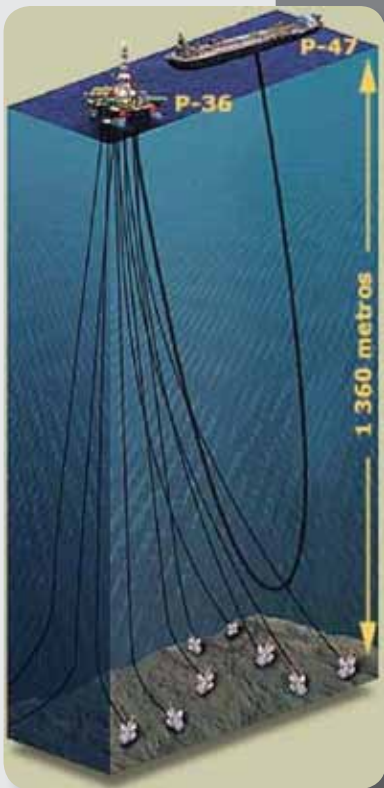
Simultaneamente, tem início a operação de retirada da tripulação da plataforma P-36 dentro de cestas carregadas por guindastes e transportados para a plataforma P-47, a 12 quilômetros da P-36, em navios-sonda e rebocadores.

Permanecem na plataforma 24 homens em funções de controle. Concluída a operação, é realizada uma chamada.

Dez homens não respondem e são considerados desaparecidos. Doze navios são deslocados para apagar o fogo.

**7h** A P-36 começa a adernar, mostrando problemas de sustentação. Os últimos homens que permanecem na plataforma são resgatados para a P-47.

**20h** A empresa interrompe as buscas aos desaparecidos até a manhã do dia seguinte.



## A PLATAFORMA

A P-36 era a maior plataforma de petróleo do mundo em capacidade de produção.

Com 112 metros de comprimento e 95 de largura, tem o tamanho de um campo de futebol.

Seus 119 metros de altura equivalem a três estátuas do Cristo Redentor.

Produzia 80 000 barris de petróleo por dia, 6% da produção brasileira e 1,3 milhão de metros cúbicos de gás natural por dia, quase a quantidade diária consumida no Estado do Rio de Janeiro.

## COMO É FEITA A PRODUÇÃO NA PLATAFORMA

Flutuando no oceano numa área com profundidade de 1 360 metros, a plataforma P-36 fica ancorada. Através de tubulações, recebe petróleo e gás natural dos 21 poços submersos. Depois de processado e tratado, o petróleo é transferido para um reservatório flutuante, a P-47, que armazena os combustíveis e os repassa aos transportadores

*Fonte (quadro): revista Veja de 21 de março de 2001*

## COMO DEVE SER A GR DAS PLATAFORMAS

Segundo o trabalho Gestão de Riscos na Operação de Plataformas de Petróleo, apresentado no V Congresso Nacional de Excelência em Gestão (Julho/2009), após o advento do acidente da plataforma P-36, “durante a operação das Unidades Marítimas de Produção é necessária a continuidade do gerenciamento dos riscos advindos das alterações e adaptações do projeto original, com o intuito de prevenir acidentes.”

A contar do início da construção de uma plataforma de petróleo, os projetos precisam ser avaliados tanto nas condições de operação quanto na visão de segurança e seus recursos de contingência.

De acordo com os autores Mauricio de Paula Oliveira da UFF e Eduardo Qualharini da UFRJ, o Gerenciamento de Mudanças é a peça-chave para prevenir acidentes ecológicos como os ocorridos com a P-36 e a

*Deepwater Horizon* sendo, portanto, fator essencial ao sucesso da Gestão de Riscos.

Com o objetivo de responder às demandas para se investigar a crescente degradação das condições de trabalho e segurança que estavam, e ainda estão, ocorrendo nas plataformas de petróleo localizadas na Bacia de Campos, tendo como resultando a ampliação e agravamento dos acidentes de trabalho, foi efetuado o trabalho Análise de causas de acidentes de trabalho nas plataformas de petróleo na Bacia de Campos, realizado na Fundação Oswaldo Cruz. Nele, os autores Carlos Machado de Freitas, Jorge Mesquita Huet Machado, Carlos Augusto Vaz de Souza.

O trabalho resultou da investigação de acidentes de trabalho nas plataformas de petróleo da Bacia de Campos, no Estado do Rio de Janeiro, no período de 18 de agosto de 1995 à 14 de abril de 1997. Nele, observa-se a necessidade de se mudar uma crença errônea na Gestão de Riscos, a de





que “a vítima é culpada até que se prove o contrário”. Segundo o texto, “quando os próprios trabalhadores acabam sendo, na maioria das vezes, responsabilizados pelos acidentes, sendo considerados culpados até que se prove o contrário, o resultado inevitável é o desenvolvimento de estratégias de gerenciamento artificial de riscos que contribuem para que os acidentes continuem ocorrendo, ainda que hajam investimentos objetivando maior controle e prevenção dos acidentes”.

Ao analisar as causas dos incidentes/acidentes, o trabalho demonstrou a classificação adotada pela empresa, para 88.31 dos 231 acidentes de trabalho registrados entre janeiro e agosto de 1996. Segundo os documentos a que teve acesso, o trabalho verificou que mais da metade dos acidentes/incidentes “ou seja 57.14% (n=132), tiveram como causa básica atitudes impróprias dos trabalhadores, vindo em seguida, com 13.85% (n=32), os relacionados a falha de projeto. A falha de manutenção correspondeu a apenas

8.23% (n=19). Em sua análise geral dos acidentes, a empresa considerou que 84.0% (n=195) corresponderam aos denominados atos inseguros, sendo o descuido, com 33.33% (n=77) e o assumir postura insegura, com 22.51% (n=52), os responsáveis por mais da metade dos denominados pela empresa “atos inseguros”, totalizando 55.84%.

Segundo os autores, as formas de classificar as questões traduzem, inevitavelmente, um determinado recorte no modo de identificá-las, analisá-las e propor estratégias de controle a partir daí. O problema, dessa visão míope da empresa, é que a forma adotada pela “além de ser extremamente limitada ao responsabilizar os trabalhadores pelos próprios acidentes em que são vítimas, não permite que se identifique os verdadeiros fatores causais que se encontram por trás dos acidentes”(quadro I abaixo).

Seguindo a mesma idéia do intitulado Gestão de Riscos na Operação de Plataformas de Petróleo, o trabalho também sugere a Gestão de Mudanças em outras palavras, quando diz que “a investigação de acidentes é um poderoso instrumento para revelar as subjacentes fragilidades da matriz sócioorganizacional das empresas em que ocorrem, permitindo vislumbrar que, para fazer uma plataforma de petróleo funcionar, por exemplo, um corpo de usos e práticas informais que não se encontravam previstas no projeto tecnológico podem, ao longo dos anos, crescer e fixar modos de operação inseguros.”

O trabalho também atenta para a questão da terceirização de mão-de-obra descomprometida com os riscos e segurança quando analisa o Quadro I, observando que este revela “que grande número dos trabalhadores acidentados pertencem as empresas contratadas, reflete a forma

**Quadro I - Distribuição dos Incidentes/Acidentes nas Plataformas de Petróleo da Bacia de Campos entre 18/08/95 e 14/04/97**

Tipo de Incidente/Acidente	Ocorrências		Trabalhadores Lesionados		
	nr	%	nr	(E/T)*	%
Acidentes	51	79,7	41**	(10/29)	95
Incidentes	10	15,6	—	—	—
Não Definidos	3	4,7	—	—	—
Total	64	100	41	—	100

Observações: (\*) Trabalhadores da empresa (E) / Trabalhadores de empresas terceirizadas (T)

(\*\*) Não foi identificada a empresa dos trabalhadores para o caso de 2 lesionados

como vem se dando o processo de terceirização de muitas das atividades operacionais pela maioria das empresas. Este processo tem com principal objetivo a redução de custos operacionais fixos, de modo a possibilitar a maximização dos lucros financeiros. A questão central é que o modo como vem ocorrendo este processo no país e na Empresa, contribui para que se ampliem e se agravem os riscos para a saúde e a vida dos trabalhadores em geral, atingindo principalmente os das empresas contratadas, os quais, comparados com os trabalhadores diretos das empresas, tendem a receberem não somente menos treinamento e informação de segurança e saúde, mas também a trabalharem em condições precárias.”

A investigação também levanta outras questões igualmente importantes como a subestima dos engenheiros responsáveis pelos projetos tecnológicos para com frequência dos incidentes que se produzem em situações anormais nos seus cálculos de confiabilidade.

Gestão de Riscos na Operação de Plataformas de Petróleo faz uma sugestão de Gerenciamento de para as Unidades Marítimas de Produção conforme o seguinte:

a) As avaliações de riscos constituem um processo de suporte e as recomendações geradas nesses estudos são fruto da percepção da equipe envolvida, a partir da aplicação de técnicas estruturadas para identificação de perigos, possuindo

caráter estritamente técnico. A implementação dessas recomendações deve ter sua viabilidade avaliada gerencialmente, a

partir da aplicação da filosofia “ALARP” (As Low As Reasonable Practicable - Tão baixo quanto razoavelmente praticável). Quando aprovadas, tais recomendações se tornam objetivos relacionados à SMS, cujo controle e provisão dos recursos necessários à sua implementação cabem ao gestor do projeto ou processo.

b) As recomendações geradas a partir dos estudos de riscos podem eventualmente inserir mudanças nas instalações e a sua implementação, portanto, deve ser gerenciada durante a fase de implantação do projeto e durante a fase de operação.

c) Os perigos relacionados à segurança das instalações, associados às falhas operacionais, devem ter seus riscos avaliados através de Análise Preliminar de Riscos.

d) Os perigos relacionados à execução das tarefas são identificados através da Análise Preliminar de Risco das tarefas, quando da emissão da Permissão para Trabalho - PT. Os riscos a eles associados são considerados, em princípio, como não toleráveis, exigindo a adoção de medidas de controle. Caso estas medidas não possam ser implementadas, as tarefas não serão realizadas.

e) A criação de um Manual de Segurança estabelece requisitos mínimos e as condutas a serem seguidas nas várias atividades de trabalho desenvolvidas a bordo das plataformas, com o intuito de minimizar os riscos identificados e prevenir a ocorrência de acidentes e incidentes.

Devemos focar nos novos projetos, ou seja, na documentação de Engenharia do projeto de uma plataforma de petróleo a ser construída. O projeto é dividido em Projeto Básico e Projeto de Detalhamento, onde em cada fase são definidos os Estudos de Riscos aplicáveis.



Após um estudo detalhado, abordando normas, técnicas e analisando os cenários atuais, a pesquisa contribui com o tema trazendo algumas respostas, conforme disposto a seguir:

1ª Questão: Os projetos podem incorporar propostas de alteração após uma análise de riscos?

Sim. As recomendações geradas a partir das análises de riscos realizadas na fase do Projeto Básico podem ser incorporadas na fase de Detalhamento do Projeto. A inclusão dessas recomendações irá depender da análise gerencial e, impacto ao prazo de término da obra e entrega da plataforma.

2ª Questão: Como é feito o levantamento dos perigos de uma plataforma de petróleo durante a sua fase de elaboração e construção?

Os estudos qualitativos são realizados através da aplicação das metodologias consagradas Análise Preliminar de Riscos – APR e Estudo de Perigos e Operabilidade – HAZOP. São elaborados com a participação dos especialistas da área operacional, de segurança e engenharia. Os estudos quantitativos de Incêndio, Explosão e Dispersão de Gases são

elaborados por empresas especializadas que utilizam aplicativos de modelagem computacional, tendo como insumo os parâmetros de processo e a geometria 3D da plataforma.

3ª Questão: Como é feito o levantamento dos perigos de uma plataforma de petróleo em operação?

Na execução das tarefas de bordo, através de uma análise prévia durante a emissão da Permissão para Trabalho, envolvendo o responsável do equipamento ou da área impactada e o executante, com o auxílio do Técnico de Segurança. Quando se tratar de alteração do projeto original, poderá haver necessidade da revisão dos estudos realizados na fase de projeto, a saber, APR, HAZOP, Incêndio, Explosão ou Dispersão de Gases, considerando a nova realidade da unidade de produção.

4ª Questão: Pode haver diferenças nos resultados das análises de riscos?

Sim. A depender do grupo indicado para participar das análises qualitativas e, no caso dos estudos quantitativos, os resultados poderão ter diferenças, devido aos softwares, insumos e critério de tolerabilidade utilizados.

**Mariana Fernandes**  
**Editora**  
sumário



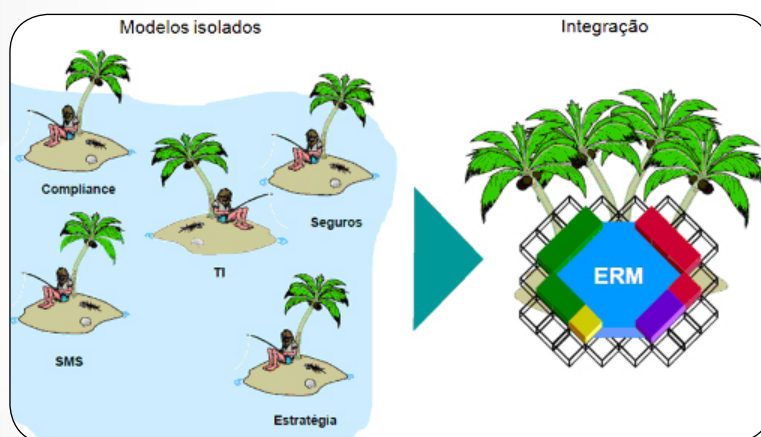
# Gestão de Riscos e a Iso 31000

Rosângela Aparecida Stringuer

Diante do cenário mundial de negócios, empresas ainda são surpreendidas por desastres naturais e por seus concorrentes, além dos problemas internos sofridos que impactam diretamente em seus resultados. No Brasil, poucas organizações dispõem de estruturas abrangentes de Gestão de Riscos, com visão holística da organização como um todo. Neste artigo irei demonstrar a importância de se ter essa estrutura.

Com o mercado mais competitivo, é clara a necessidade das organizações conhecerem seus riscos em todos os níveis e, para que isso aconteça, é necessário haver uma área de Gestão de Riscos que integre todas as áreas de cada organização.

O objetivo da área é tratar as informações de forma agrupada, cruzando a influência de uma atividade na outra. Áreas gerenciais devem ter braços operacionais trabalhando de forma unificada para que o nível estratégico tenha acesso a informações plausíveis para tomada de decisões, em outras palavras, o nível estratégico deve enxergar de forma clara suas exposições operacionais.



Fonte: ABNT – Associação Brasileira de Normas Técnicas.

Dentro desse enfoque, a área de Gestão de Riscos, obrigatoriamente, deve abranger inúmeras disciplinas, já que há atividades administrativas comuns à todas as áreas da empresa.



Dessa forma, esta área deve possuir um processo sistêmico e contínuo, embasado nas melhores práticas e na norma de Gestão de Riscos ISO 31000.

A ISO 31000 descreve claramente que convém às organizações realizar o seguinte processo.

## 2 - ESTABELECIMENTO DO CONTEXTO

Entendimento dos fatores internos e externos, ou seja, as variáveis incontroláveis. Nos fatores internos, procura-se entender os objetivos estratégicos da organização, cultura, processos, estrutura e sua estratégia.

## 3 - IDENTIFICAÇÃO DE RISCOS

Listagem dos perigos e suas fontes/causas.

## 4 - ANÁLISE DE RISCOS

Compreensão dos riscos utilizando os critérios de probabilidade e consequência (impacto).

## 5 - AVALIAÇÃO DE RISCOS

Tem o objetivo de auxiliar na tomada de decisões. Busca saber através dos critérios estabelecidos, quais riscos serão tratados.

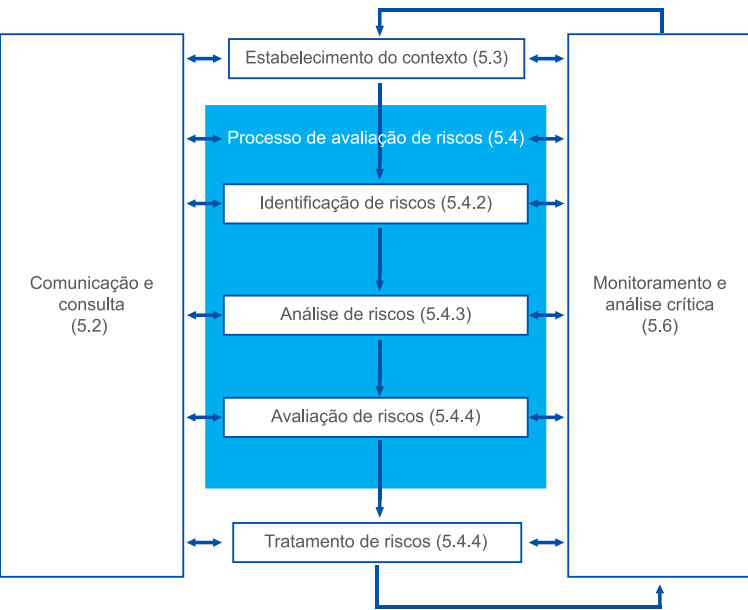
## 6 - TRATAMENTO DE RISCOS

Processo contínuo. Realização de investimentos: recursos humanos, recursos tecnológicos e recursos organizacionais (processos), nunca deixando de reavaliar os riscos tratados, considerando as mudanças no contexto interno e externo, caso seja necessário.

## 7 - MONITORAMENTO E ANÁLISE CRÍTICA

Checagem periódica das ações tomadas. É necessário estabelecer responsáveis.

Esse processo deve ser conduzido por toda organização, tendo como principal objetivo identificar e medir os riscos para as tomadas de decisões. De acordo com



### Framework da ISO 31000.

A norma pode ser aplicada em todo tipo de organização, independentemente do tipo, tamanho ou ramo de atuação. Por essa razão, possui uma abordagem genérica, fornecendo apenas os princípios e diretrizes, não determinando o “como fazer”, deixando sob a responsabilidade de cada organização estabelecer seus próprios critérios. Abaixo, uma breve explanação das fases do framework da ISO 31000.

### I - COMUNICAÇÃO E CONSULTA

Comunicação interna e externa. Objetivo de assegurar que os responsáveis e partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e suas respectivas razões.



seu apetite ao risco, item que, de acordo com a ISO 31000, convém à organização definir, a organização pode decidir em: monitorar o risco, aceitar o risco, transferir o risco ou tratar o risco. Com base na decisão, a organização emprega seus investimentos de forma mais efetiva, possibilitando o fortalecimento e eficiência econômica, o que impacta diretamente em sua posição competitiva perante seus concorrentes.

## CONCLUSÃO

Os recentes eventos e desastres pelo mundo mostram às organizações a necessidade de gerenciar seus riscos. Podemos nos perguntar, quantas organizações foram afetadas com as chuvas do início deste ano no Rio de Janeiro? Quantas organizações foram afetadas no 11 de setembro? Passados nove anos, boa parte as organizações evoluíram na questão, mas, infelizmente, boa parte ainda é pega de surpresa. Ou os riscos serão gerenciados ou continuaremos apostando na sorte.

**Rosângela Aparecida Stringuer**

Consultora da Brasiliano & Associados

*sumário*



# Serviços de Outsourcing

**Tire o peso de suas costas !  
Deixe para quem é ESPECIALISTA!!**

Outsourcing é a terceirização do processo de gestão de riscos e da segurança empresarial. O escopo inclui o planejamento, a implantação e a administração de todos os serviços e processos terceirizados.

## VANTAGENS DO OUTSOURCING:

- Mão-de-obra especializada
- Melhoria da qualidade do serviço
- Otimização de recursos
- Aumento da produtividade
- Liberação da estrutura da empresa para sua atividade fim
- Simplificação da estrutura interna
- Redução de ação trabalhista
- Agiliza decisões e ações



**Consulte – nos!!!**

informações | 11 5531-6171  
| [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)



# 31010 e Brasileiro

## Técnicas e Ferramentas de GR pelo Criador do Método Contemplado

Antonio Celso Ribeiro Brasileiro



Brasiliano é autor do método que será incluso na próxima revisão da ISO/IEC 31010:2009 “Risk management – Risk assessment techniques” ou, em português, Gestão de riscos – Técnicas de avaliação de riscos.

Considerada pela maioria dos gestores brasileiros a melhor ferramenta de análise de riscos, o Método Brasileiro deve constar na tabela de técnicas e ferramentas da 31010 em sua nova edição.

E, para atualizar você leitor quanto à recém-lançada 31010, Brasileiro explica, a seguir, os principais pontos da norma de apoio à 31000, que fornece diretrizes detalhadas sobre critérios de seleção e aplicação de várias técnicas qualitativas e quantitativas para a avaliação de riscos.

### **O conhecimento das normas ISO Guia 73 e ISO 31000 são necessários e ou prévios à compreensão da 31010?**

Claro que são necessários. A ISO Guia 73 é uma norma que dá o vocabulário, então ela está padronizando para o mundo, o que é muito importante, a questão da semântica e vocabulário. Ou seja, ela padroniza o que vem a ser uma análise de risco, uma gestão de risco, probabilidade... Então todo mundo passa a ter o mesmo entendimento. Antigamente tinha o que o brasileiro falava, o que o “Zezinho” comentava, o que a norma australiana falava, o que a norma da Hojas falava, o que o COSO falava. Agora temos uma norma internacional, reconhecida mundialmente, por consenso, onde se padronizou a nomenclatura. Já a ISO 31000, fornece o framework, os passos para se estar executando uma gestão de risco, ou seja, um processo igual o PDCA, de gestão, onde se fecha o ciclo fazendo um processo retroalimentativo. Essa é a grande sacada da 31000. Ela cita quais são os passos e ela te obriga a utilizar ferramentas. Quais ferramentas se irá utilizar, é critério da empresa. Para orientar na escolha dessas ferramentas foi lançada



a 31010, que dispõe as ferramentas que poderão ser utilizadas ou que a ISO recomenda, ou que o mundo colocou como “melhores práticas”, é o que contém a 31010. Então ela usa o framework da 31000 e usa técnicas específicas de análise de risco, para cada uma dessas que estão lá colocadas, a norma explica a melhor aplicabilidade de cada uma. Então, por exemplo, para se fazer uma identificação de risco, você pode utilizar Brainstorming, um questionário via delphi. Quem vai escolher a melhor ferramenta será o consultor, o técnico da empresa.

Outro exemplo, quanto à escolha do método, quantitativo ou qualitativo, a 31010 não impõe um ou outro. É a empresa que deve escolher. O que ela diz é quais ferramentas estão disponíveis para cada método, dando dicas de quais a empresa pode utilizar.

### **A norma está excluindo alguma técnica ou ferramenta considerada ultrapassada?**

Não, não excluiu nenhuma. A norma mostra todas que tem no mundo e deixa à disposição para que as pessoas possam estar utilizando as que melhor se encaixem no seu negócio. Faltou a Matriz SWOT que está orientada na Ferma (*Federation of European Risk Management Association*). Mas a norma ainda vai ter modificações em suas próximas revisões.

### **Qual será a periodicidade de revisão da 31010?**

Bi-anual. (A ISO 31010 entrou, oficialmente, em vigor no último dia 1o. de dezembro de 2009. Mas a ABNT NBR ISO/IEC 31010, em português, ainda não tem data definida para ser publicada.)

### **A norma trouxe técnicas novas ou apenas selecionou as melhores já em uso pelas empresas?**

Colocou apenas as que já são utilizadas. E dá uma tabelinha de aplicabilidade (vide abaixo), que é a grande sacada da norma, que traz mais ou menos 35 processos e ferramentas de avaliação de risco. Na tabela, a 31010 separa o que serve para fazer Identificação de Risco, fazer Análise de Risco, definir Nível de Risco e fazer Avaliação de Risco, sendo que as ferramentas a serem escolhidas ficam sob decisão da empresa.

Tabela A1 - Seleção de Ferramentas e Técnicas para Avaliação de Riscos						
Ferramentas e técnicas		Processo de avaliação de riscos				
		Identificação de Riscos	Análise de Riscos			Avaliação de Riscos
			Consequência	Probabilidade	Nível de Risco	
1	Análise de Modos de Falha e Efeitos (IEC 68012)	AA	NA	NA	NA	NA
2	Análise Crítica de Modos de Falha e Efeitos (IEC 68012)	AA	AA	AA	AA	AA
3	Análise de Árvore de Falhas (IEC 61025)	A	NA	AA	A	A
4	Estudo de Perigos e Operabilidade (HAZOP)	AA	AA	A	A	A
5	Manutenção centrada em confiabilidade (IEC 60300-3-11)	AA	AA	AA	AA	AA
6	Análise de Markov (IEC 61665)	A	AA	NA	NA	NA
7	Análise de Confiabilidade Humana	AA	AA	AA	AA	A
8	Análise Preliminar de Perigos (APP)	AA	NA	NA	NA	NA
9	Análise de Árvore de Eventos (ETA)	A	AA	A	A	NA
10	Brainstorming	AA	NA	NA	NA	NA
11	Entrevistas Estruturadas ou Semi-Estruturadas	AA	NA	NA	NA	NA
12	Técnica de Delphi	AA	NA	NA	NA	NA
13	Checklists	AA	NA	NA	NA	NA
14	Matriz de Probabilidade/Consequência	AA	AA	AA	AA	A
15	Análise de Camadas de Proteção (LOPA)	Aw	AA	A	A	NA
16	Técnica Estruturada de What If? (SWIFT)	AA	AA	AA	AA	AA
17	Análise de Árvore de Decisões	NA	AA	AA	A	A

Tabela A1 - Seleção de Ferramentas e Técnicas para Avaliação de Riscos							
Ferramentas e técnicas		Identificação de Riscos	Processo de avaliação de riscos			Avaliação de Riscos	
			Consequência	Probabilidade	Nível de Risco		
18	Análise de Gravata Borboleta	NA	A	AA	AA	A	
19	Simulação de Monte Carlo	NA	NA	NA	NA	AA	
20	Análise de Causa Raíz (RCA)	NA	AA	AA	AA	AA	
21	Análise de Perigos e Pontos Críticos de Controle (HACCP)	AA	AA	NA	NA	AA	
22	Avaliação de Riscos Ambientais	AA	AA	AA	AA	AA	
23	Análise de Cenários	AA	AA	A	A	A	
24	Análise de Impacto nos Negócios (BIA)	A	AA	A	A	A	
25	Análise de Causa e Consequência	A	AA	AA	A	A	
26	Análise de Causa e Efeito	AA	AA	NA	NA	NA	
27	Análise de Circuitos Ocultos	A	NA	NA	NA	NA	
28	Estatística Bayesiana e Redes de Bayes	NA	AA	NA	NA	AA	

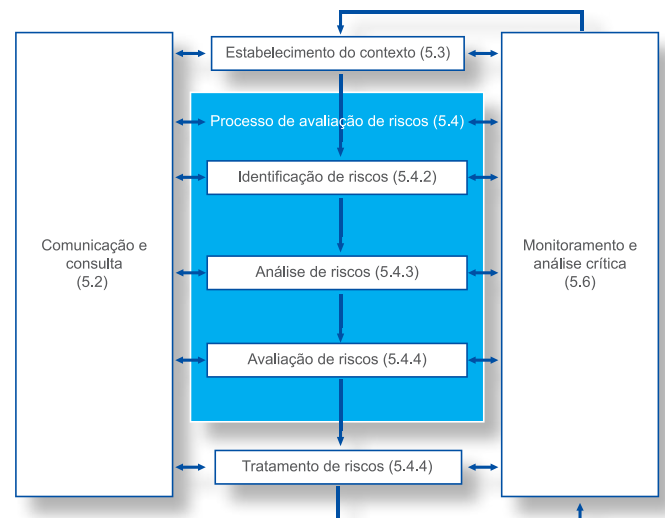
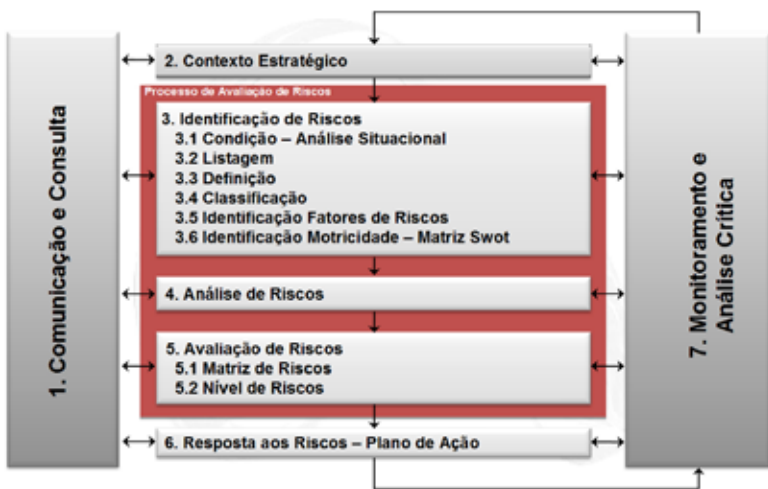
(A tabela acima foi traduzida da ISO/IEC 31010. Ela mostra como uma determinada técnica se aplica em cada etapa do processo de avaliação de riscos, definida como Altamente Aplicável, Aplicável ou Não-Aplicável.)

### Qual o know-how necessário para que o gestor compreenda o texto da norma?

O gestor vai ter que ter experiência e vai ter que ter um conhecimento prévio amplo, porque o texto cita as ferramentas de maneira genérica, já que essas são dadas apenas como referência.

### Quais são as técnicas contidas no Método Brasileiro e contempladas pela 31010?

Tem a Matriz de Risco, o Brainstorming, o Método Delphi, Cenários e o Diagrama de Causa e Efeito.



---

### **A aplicação de técnicas sistemáticas de avaliação de riscos são sucintamente descritas na norma ou são apenas citadas?**

Somente descritas. A norma não mergulha profundamente em cada uma delas, dá apenas a explicação. Mas, coloca todas. Até o BIA (*Business Impact Analysis*), utilizado na continuidade de negócios é citado na norma. São mais ou menos duas ou três páginas por técnica.

---

### **Por que deve haver uma técnica diferenciada para cada fase do processo de avaliação de riscos?**

Não é uma técnica diferenciada. Cada ferramenta se aplica melhor dentro do framework da ISO 31000. Ou seja, como é que se faz para identificar o risco? Pode-se trabalhar através de um questionário, de um *check-list*, de um brainstorming...mas qual é a melhor dessas três? As três são boas quem decide isso é a empresa. E se a empresa perguntar para o gestor por que ele está usando tal ferramenta em vez de outra ele pode falar que selecionou a melhor para a necessidade e formato da empresa e com base na 31010. Dito isso não há mais o que questionar, já que o que consta na norma são técnicas oficiais e não meramente aleatórias.

---

### **As técnicas qualitativas e quantitativas contidas estão misturadas ou separadas na 31010?**

Estão separadas.

---

### **A norma estabelece algum critério para a utilização das técnicas qualitativas ou quantitativas?**

Não, critério nenhum. Fica a critério da empresa. A 31010 sugere que se utilize para questões de impacto não somente a parte financeira mas também a parte de imagem, de recursos humanos, a relativa à área operacional. Ela veio dizer quais são as ferramentas que o mundo está utilizando, explicando-as. A Ferma, que é a norma europeia, só cita

---

### **A orientação sobre a seleção das melhores técnicas para as fases do processo de avaliação de riscos ela fornece somente através da tabela?**

Somente através da tabela onde ela dá como sugestão. As ferramentas selecionadas foram resultado de reuniões onde se estabeleceu um consenso entre 35 países. A norma traz, inclusive, os atributos da seleção das ferramentas.

---

### **Qual a importância de as organizações padronizarem não apenas os conceitos mas também as técnicas empregadas na Gestão de Riscos?**

A importância está em as organizações estarem utilizando uma mesma ferramenta para a empresa inteira. Mas isso talvez não seja possível, talvez seja “um sonho de uma noite de verão”, porque às vezes para uma área de segurança do trabalho você pode estar utilizando uma ferramenta e na segurança corporativa outra e na parte de fraudes outra ainda, que mais se adéque. Um ponto importante a ressaltar é que o framework e a Matriz de Risco têm que ser iguais. Não pode haver mais de uma Matriz de Risco dentro da empresa.



---

## **Como uma consultoria especializada em Gestão de Riscos trabalha para implementar a 31010 numa organização?**

Então, não é a 31010. Nós estaremos implementando a 31000 utilizando as ferramentas da 31010. Porque a 31000 traz o framework para utilizar o ferramental da 31010. Então ela não é uma norma de implantação, é orientativa.

---

## **A 31000 será um dia certificadora?**

Acho que, no futuro, vai. Quando sair a parte 2 da 31000 essa trará os requisitos para a certificação. Por enquanto ela é orientativa e “guarda-chuva”.

---

## **Faz parte do processo primeiro promover o conhecimento da área e depois certificar?**

Isso mesmo. A de continuidade de negócios, por exemplo, já foi publicada em duas partes, sendo a parte um o código de prática e a parte dois os requisitos para certificação.

**Mariana Fernandez**

Editora

sumário





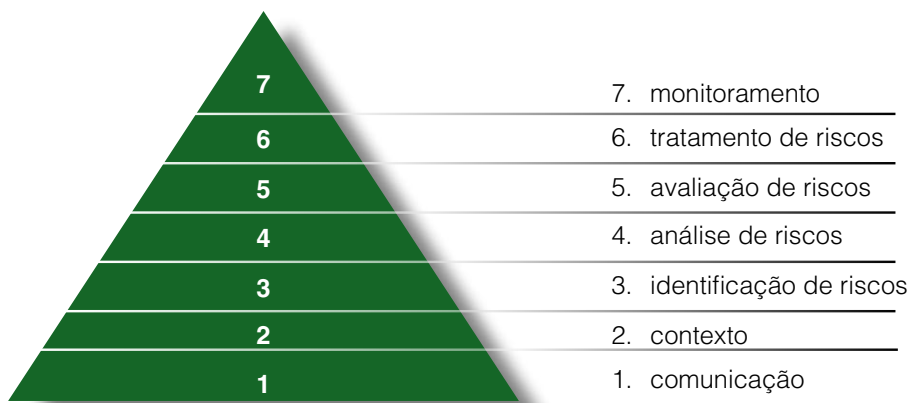


## Serviços de Consultoria **Plano de Gestão de Riscos Corporativos - PGRC**

### **Sua empresa conhece o TAMANHO de seus riscos??**

Um PGRC é um processo estruturado para que a empresa possa identificar eventos que expõem os objetivos da organização.

O processo de Gestão de Riscos, hoje é estruturado com base na ISO 31000.



**A Brasiliano pode ajudar você a elaborar seu plano de PGRC  
Consulte – nos!!!!**



# O Papel da Área de Gestão de Riscos nas Empresas

*Renato Vial Polidori*

O papel da área de Gestão de Riscos nas empresas é estudar os aspectos inerentes aos riscos, ameaças e vulnerabilidades, para que se possa fazer a prevenção de segurança nos sites da empresa.

Dentro desses aspectos, pode-se dizer que uma área de Gestão de Riscos exerce, na prática, vários papéis dentro de uma empresa, a saber:

- **Papel Orientativo** – desempenhado quando a área analisa os contextos dos riscos, ameaças e vulnerabilidades e compatibiliza-os com as medidas de proteção (segurança) adequadas orientando a empresa sobre como portar-se frente a essas situações. Este papel é extremamente importante, pois é a partir dele que serão definidos e desenvolvidos os projetos e o planejamento de segurança e de gestão de riscos da empresa.
- **Papel Educativo** – neste papel a área de Gestão de Riscos atua em contato direto com os colaboradores da empresa no sentido de conscientizá-los e comprometê-los com as melhores práticas de segurança frente aos riscos analisados e presentes na realidade da empresa. Também como o papel anterior, tem grande importância pois é com a conscientização e o comprometimento das pessoas que se conseguem as

adesões necessárias ao sucesso dos planos e das medidas de segurança e de gestão de riscos implementadas na empresa.

- **Papel Administrativo** – ocorre quando a área de Gestão de Riscos atua como uma área de “gestão” efetiva dos riscos e das medidas de proteção implementadas. Neste é que a área se posiciona como gestor / administrador das políticas de segurança existentes, zelando por suas perfeitadas difusões, praticabilidades, atualizações e manutenções. Tanto quanto os demais papéis, este papel é de grande importância por revestir a área de poderes de esclarecer, determinar, sancionar, enfim exercer todas as funções administrativas frente aos riscos determinados pela organização e as medidas necessárias para sua gestão, evitando, enfim, impactos danosos à organização.

Importante ressaltar que quando se fala em Gestão de Riscos, sob a ótica administrativa, deve-se primeiramente ver que quando uma área tem um risco, ela pode administrá-lo risco adotando uma das seguintes posturas:

- Aceitar o risco.
- Evitar o risco.
- Minimizar o risco.
- Desviar/transferir o risco.

Discorrendo um pouco melhor, as possibilidades de gestão de riscos exercidas pela área podem ser resumidas da seguinte forma:

- Aceitar o risco quando a área de gestão

de risco está ciente do risco que se oferece para sua empresa.

- Evitar o risco: quando a área de gestão de risco numa empresa está ciente do risco apresentado e busca fazer com que quando o risco ocorra não atinja a empresa.
- Minimizar o risco: quando a área de gestão de risco numa empresa sabe que há um risco em um determinado ponto de situação e busca fazer com que quando ocorra o sinistro, aconteça o mínimo possível.
- Desviar o risco: quando uma empresa, por exemplo, apresenta um risco para um fornecedor / prestador de serviço e a empresa cliente faz um documento no qual caso o sinistro que foi descrito ocorra, a empresa que está fornecendo o serviço saiba que o risco não é mais do cliente e sim dela.

Pensando de maneira prática, por exemplo, existem empresas onde todos os novos colaboradores passam por uma palestra/treinamento onde são informados sobre qual é o papel da segurança na empresa; quais as principais posturas esperadas pela organização de seus colaboradores frente aos riscos, o que existe nas normas internas, enfim, nesse tipo de evento os colaboradores recebem a devida orientação sobre o papel da área e o seu papel frente aos aspectos de segurança. Isto é parte do papel educativo sendo colocado em prática.

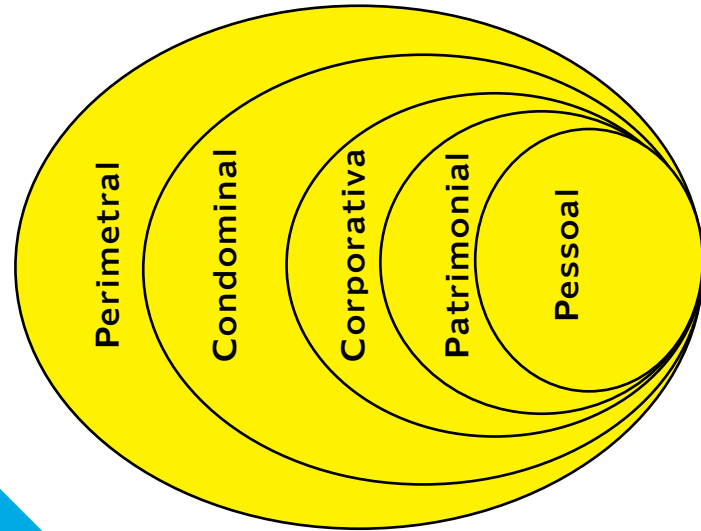
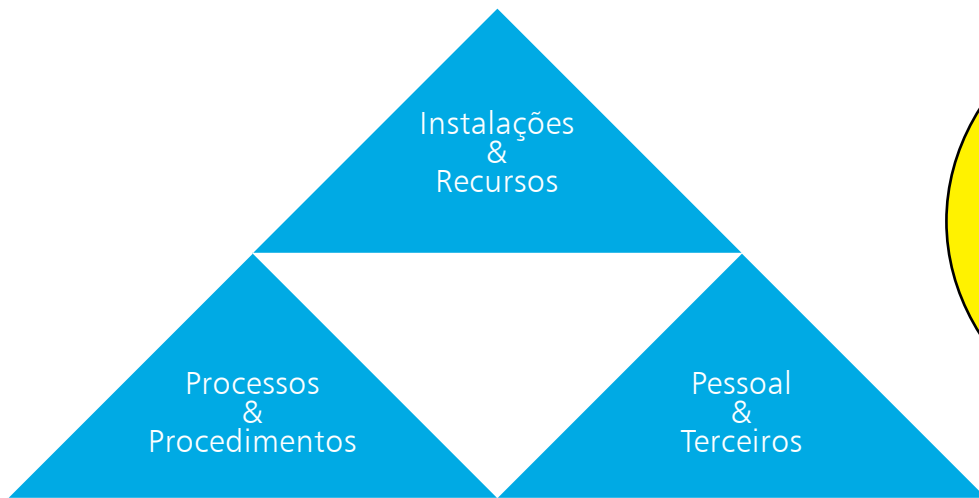
Já quanto a área que atua em aspectos de Análise Preventiva de Riscos para Ambientes (Instalações e Recursos), Processos e Procedimentos e Pessoas e Terceiros, o papel em questão é de ordem Orientativa.



Nesse tipo de papel a área, através de sua expertise, analisa contextos, ameaças, vulnerabilidades e finalmente os riscos provenientes dessas situações e recomenda as medidas de proteção (segurança preventiva) que permitirão à organização controlar e gerir seus riscos adequadamente.

de políticas e diretrizes de segurança que enxerguem desde a parte mais externa da organização (segurança perimetral) até a parte mais interna que é a segurança para pessoas.

O diagrama abaixo dá uma idéia disso:



Já sob a ótica administrativa, cabe à área de Gestão de Riscos exercer o papel de guardião das normas e da praticabilidade das mesmas dentro da organização.

Nesse sentido, atua junto aos colaboradores desde a parte de desenvolvimento e execução de Programas de Conscientização e Comprometimento, passando pelas políticas de segurança, diretrizes, normas e procedimentos e ainda chegando aos aspectos de monitoria, aplicabilidade, métricas de aceitação e uso, conhecimento pelos colaboradores, etc.

Ainda nesse papel, a gestão de riscos deve estar atenta às mudanças de perfis e/ou de contexto da empresa, do mercado e/ou dos riscos existentes para que possa atuar sempre em conformidade com aspectos reais, atualizados e em abordagens práticas e consistentes.

Um exemplo típico do aspecto administrativo da gestão de riscos é a elaboração

Em resumo, o papel da área de gestão de riscos nas empresas é trazer a segurança, bem estar e conforto para a organização. Isso, ela consegue através do exercício de vários papéis dentro da empresa, todos eles importantes e que se complementam entre si, mas que fundamentalmente atendam às necessidades da organização.

Com isso podemos concluir a filosofia de segurança que diz:

“A melhor segurança não é aquela que necessariamente é vista, mas sim aquela que é sentida”.

**Renato Vial Polidori**

sumário



# ACONTECE

na *Brasiliano*

Mariana Fernandez

## **RISKVISION** online

O software Risk Vision, uma ferramenta de gestão e análise de riscos corporativos, lançada na Exposec 2010, já está disponível para compra no site da Sicurezza Editora no link [www.sicurezzaeditora.com.br/risk-vision/](http://www.sicurezzaeditora.com.br/risk-vision/).

Destinado para consultores, empresas de serviços, indústrias, estudantes, gerentes, coordenadores e supervisores de segurança, a ferramenta é o que qualquer gestor de riscos precisa para elaborar seus projetos de GRC com tecnicidade.

### **PCN - prevenir (com quem entende) é melhor do que remediar**

Este ano a Brasiliano & Associados está atendendo uma grande demanda de clientes que visam executar planos de continuidade de negócio, o famoso PCN.

Com metodologia própria e a vasta experiência a B&A já executou diversos projetos em diferentes ramos de atividade, tais como: bancária, indústria farmacêutica, sistemas de informação, energia, etc.



Segundo a consultora Sandra Alves, no ambiente de continuidade de negócio, uma das mais importantes tarefas realizadas é o BIA (Business Impact Analysis), já que consiste no mais importante referencial para o desenvolvimento da Estratégia de Continuidade de Negócio.

Na etapa Estratégia de Continuidade de Negócio, ocorre a escolha dos métodos alternativos de operação a serem usados após uma interrupção, para manter os processos críticos de negócios da organização identificados através do BIA (Business Impact Analysis).

Sandra Alves, ressalta algumas das estratégias possíveis de serem empregadas, como por exemplo:

- Manter espaço dedicado – tipo de estratégia que proporciona disponibilidade imediata do site de contingência e garantida, mas é mais caro do que o espaço compartilhado.

- *Os colaboradores devem trabalhar remotamente – tipo de estratégia que requer planejamento e disponibilidade da infraestrutura adequada.*
- *Espaço compartilhado – tipo de estratégia que proporciona acesso rápido, possuindo um investimento menor, e que deve ser utilizada quando os departamentos clientes, estão localizados em lugares diferentes e expostos a perigos relativamente diversos, porém sua disponibilidade não pode ser absolutamente garantida e demora mais para tornar-se produtiva.*
- *Utilização de espaços existentes na companhia – tipo de estratégia que envolve a mudança de atividade de funcionários que executam processos menos críticos, para a execução daqueles que têm uma prioridade elevada (processo crítico).*

*A consultora da B&A explica que dentre os tipos de estratégia aplicados pela B&A, “há casos de instituições bancárias, que possuem áreas muito críticas, até mesmo regulamentadas, como por exemplo, a tesouraria, cabendo manter como estratégia de continuidade, um espaço dedicado que é destinado a atender os processos críticos que não podem parar até 04 horas, e que causam impactos severos e catastróficos”.*

*“Dentro do contexto de estratégia, temos clientes na área de indústria, que possuem um site original e diversas regionais espalhadas por todo o Brasil, e caso ocorra uma descontinuidade as áreas críticas do site original ocupam como site de contingência suas regionais, assegurando a continuidade de suas atividades, ou seja, o chamado espaço compartilhado”, conta Sandra.*

*A especialista em PCN ressalta que o segredo para garantir a continuidade dos negócios consiste na compreensão da empresa de um aspecto geral com a posterior determinação de seus processos críticos, aliadas à estratégia de continuidade que melhor se aplique e à pessoas devidamente treinadas.*

*Para saber mais sobre PCN, entre em contato com a Divisão de Consultoria da B&A.*

**sumário**

# Uma Nova Categoria de Risco: A Inércia

André Pitkowski

Uma avaliação de riscos de TI criteriosa é essencial para o contínuo desenvolvimento de um ambiente de TI que trabalha baseado na relação custo/benefício. Infelizmente, as ferramentas e os frameworks de análise de riscos de TI muitas vezes apresentam apenas indicadores de grande visibilidade, tais como o número de operações, o impacto financeiro direto, ou a eficácia na recuperação de desastres e continuidade de negócios em toda a empresa. Esses indicadores tradicionais são importantes e válidos para a avaliação de riscos.

Este artigo explora o conceito de que o risco de TI também é suportado por um fator mais abstrato, mas potencialmente forte: o nível da organização que está comprometido com sistemas ágeis. O termo “ágil” é usado aqui no sentido estratégico, como a capacidade de readaptar a empresa com rapidez e eficiência frente a novos negócios (aquisições e fusões), regulamentações e mudanças técnicas.

George Westerman e Richard Huntsman, em seu livro de *Risco de TI*, distribuem os riscos de TI em quatro categorias: disponibilidade, acesso, precisão e agilidade (os quatro “As” em inglês). Enquanto a maioria das análises de risco e de auditoria de TI incluem somente as três primeiras categorias, o grau de agilidade da empresa é muitas vezes ignorado, apesar da sua importância estratégica para o sucesso contínuo da organização.

Agilidade é a capacidade da organização de responder adequadamente às necessidades de negócio da empresa, e pode ser considerado o termo mais “vago” das quatro categorias de risco, mas também pode ser o mais importante a partir da perspectiva de entrega de resultados no dia-a-dia da operação.

## A EVOLUÇÃO DA GESTÃO DE RISCOS

A recente crise mundial de 2008 chamou a atenção sobre os métodos para se controlar, regular e atenuar os fatores de risco, incluindo, mas

certamente não limitado às operações de crédito e a volatilidade do mercado. Essa atenção é apenas a mais recente manifestação dos esforços de gestão de risco que têm acontecido nos últimos 70 anos.

Os Acordos de Basiléia (I e II), que definem padrões mundiais para as reservas das instituições financeiras de capital de risco, são exemplos recentes do esforço global de redução de risco. As práticas de avaliação de risco têm evoluído em sofisticação, complexidade matemática e detalhamento.

Como é que essa nova e revigorada cultura de gestão de riscos afeta hoje o dia-a-dia da avaliação de riscos para um auditor de TI? Claro que as maiores expectativas do trabalho do auditor de TI se voltam para a gestão de TI. Por exemplo, o *Chief Information Officer* (CIO) pode procurar por uma visão mais estratégica dos riscos de TI, com base em um entendimento do negócio da organização e da direção da tecnologia. As perguntas podem incluir os seguintes tópicos:

Como os riscos podem ser quantificados de forma mais eficaz?

Existe uma maneira prática de se educar o resto da organização, especialmente a alta administração, em longo prazo, em questões mais estratégicas?

Como pode o risco ser tratado através de uma abordagem mais integrada e não simplesmente como uma série de ameaças independentes?

Existe uma maneira de se quebrar o paradigma de risco isolado, abordada de modo externo à organização ou através de soluções pontuais?

## RISCO ESTRATÉGICO X RISCO TÁTICO

O enfoque tradicional de análise de riscos de TI tem sido visível nos eventos táticos. Em termos do modelo Westerman-Huntsman,

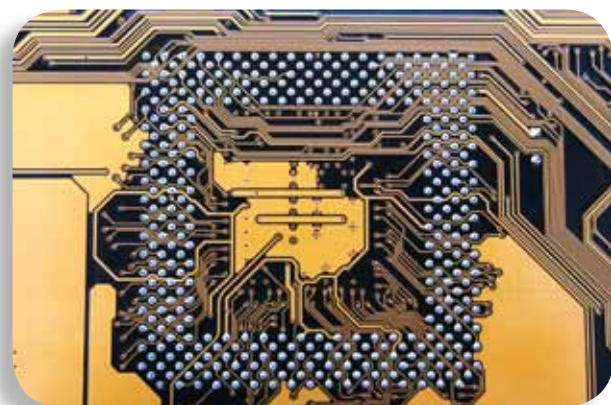
esses eventos incluem falhas na disponibilidade de recursos de computação, acesso inadequado e processamento impreciso. Claro que a mitigação desses riscos conhecidos é essencial para a continuidade dos negócios de qualquer organização.

No entanto, os riscos em longo prazo e de lento desenvolvimento, como a falta de manutenção de sistemas, por exemplo, podem apresentar prejuízos significativos em determinado momento para a rentabilidade e eficiência das operações. Agilidade no tratamento de riscos é estratégica e se desenvolve ao longo do tempo. Pode não ser imediatamente visível e, portanto, pode ser mais difícil de avaliar e de se apresentar à gestão.

A falta de agilidade (inércia no processo) afeta diretamente a habilidade da organização para responder às alterações técnicas, regulatórias e de concorrência no mercado. Inércia no tratamento destes riscos pode vir do nível mais baixo da organização, aquele chamado de “porcas e parafusos, tubos e conexões, os bombeiros, ajudantes de pedreiros ou equipe Bombrill”, subindo até estruturas organizacionais estratégicas impróprias ou inapropriadas.

Na extremidade inferior, por exemplo, um programa legado pode ter sido codificado com centenas de declarações *go-to*. Ele pode funcionar perfeitamente (depois de muita depuração), mas se tiver de ser alterado, a probabilidade de um fracasso é muito alta. Práticas de programação ruins impactam diretamente os sistemas, que tornam-se lentos e não ágeis.

No outro extremo do espectro, uma organização com alto risco de inércia estratégica





pode ter suas aplicações executadas em silos e desconectadas, com um número excessivo de ligações interorganizacionais e com capacidade limitada de alterar uma funcionalidade de TI dentro de um prazo razoável.

## **QUANDO A ÚNICA CONSTANTE É A MUDANÇA: O VALOR ESTRATÉGICO DA AGILIDADE**

Na década de 1990, muitas organizações progressistas implementaram sistemas de *workflow* como um componente importante de sua estratégia de gestão de processos de negócios. Os benefícios foram e continuam a ser claros: circulação de informações de forma estruturada, com trilhas de auditoria, procedimentos de autorização simples e a capacidade de fornecer caminhos alternativos se os recursos estiverem temporariamente indisponíveis.

Em um planejamento de recursos empresariais da Oracle (ERP), por exemplo, o fluxo de ordens de compra de um iniciador de nível inferior flui para um aprovador de alto nível se o montante for superior a um valor predefinido, enquanto que para outras etapas da compra, segue o clique normal para pagamento. Em um sistema de controle de mudanças, a implementação de uma mudança de programa não pode ser colocada em produção até que um usuário / autorizador aprove eletronicamente a mudança.

Em contraste com os dias de hoje, empresas com e sem fins lucrativos estão cada vez mais obrigadas a ir além do hierárquico, um passo de cada vez em procedimentos adaptados para sistemas de *workflow* (ainda que estes sistemas continuem a desempenhar um papel vital em muitos processos core).

No mercado, a mudança está ocorrendo numa taxa de crescimento exponencial. Os clientes têm a disponibilidade da web, podendo aproveitar muito mais do que antes, suportados pela flexibilidade para mudar de fornecedor com facilidade. Assim, para muitas empresas, a capacidade de mudança e a possibilidade serem as primeiras no mercado é, muitas vezes, mais importante do que a capacidade de produzir barato, com práticas padronizadas.

A interrupção de disponibilidade de serviço não é mais um evento ocasional. Agora a ruptura é quase constante. Só as empresas ágeis conseguem mudar produtos, ofertas, serviços e fornecedores com a rapidez suficiente para manter ou aumentar sua quota de participação de mercado. Cada vez mais, são as ações rotineiras que geram as vantagens competitivas.

Assim, as organizações com sistemas e processos de TI ágeis irão prosperar mais em relação a outras organizações, enquanto a tecnologia, as condições de mercado, as regras governamentais e outros fatores tendem a tornarem-se mais perturbadores no dia-a-dia do negócio.

## **O CAMINHO PARA A AGILIDADE**

Uma plataforma de software forte, uniforme, estável e previsível pode ser o elemento mais importante de uma organização de TI no programa de redução de risco. E, enquanto uma plataforma forte (software, hardware e metodologias), afeta todas as áreas de riscos de TI, tem ao mesmo tempo um efeito desproporcional sobre o risco da inércia (falta de agilidade). Infelizmente, não existe uma fórmula simples





para alcançar a flexibilidade que a maioria das empresas necessita para responder às rápidas mudanças.

As empresas com visão de futuro, que pretendem maximizar a agilidade e promover o intercâmbio de idéias, usufruindo da tomada de decisão não hierárquica e da plena utilização do espaço mental de toda a organização (incluindo funcionários, contratados, fornecedores e clientes), muitas vezes, promovem a agilidade com ferramentas de interação humana.

Exemplos dessas ferramentas (a maioria se encontra sob a égide da web 2.0) incluem pacotes de colaboração, softwares de compartilhamento de informações (tais como o SharePoint da Microsoft), wikis, blogs, sistemas de alerta, serviços hospedados para mudanças rápidas, redes sociais e até mesmo *mashups*.

Algumas organizações têm até usado os ciclos de ociosidade de milhões de PCs de voluntários para ajudar nas tarefas de resolução de problemas complexos. Um exemplo é o projeto *Folding @ home*, que prevê três pesquisadores da área médica com o equivalente a um supercomputador para resolver problemas complexos de dobramento de proteínas.

Uma organização sem esses recursos (que seja sem parte deles) corre o risco de reagir atrasada (inércia) aos seus clientes ou às condições de mercado. Em seu livro *Dot Cloud: A 21st Century Business Platform Built on Cloud Computing*, Peter Fingar observa que as empresas tradicionais não são apenas dramaticamente assimétricas em termos de compensação, mas também na disponibilidade de informações.

Funcionários podem estar desinformados sobre o negócio, conhecimento das atividades de outras equipes e não sabem

qual é a visão clara sobre a direção da empresa. Altos executivos podem (mas nem sempre) ter acesso a vastas quantidades de informações detalhadas e dados sumarizados (por exemplo, relatórios de *Business Intelligence*), enquanto os funcionários de nível inferior se encontram muitas vezes quase no escuro.

Organizações do futuro devem confiar na computação distribuída, aproveitando a inteligência e conhecimento de vários grupos, incluindo funcionários, fornecedores, clientes e outras pessoas e até nas comunidades de interesse relevante.

## **FOCO EXCESSIVO NOS RISCOS VISÍVEIS**

Existe uma velha piada sobre um bêbado que está rodopiando em torno de um poste de luz procurando as chaves do carro. Quando perguntado por que ele está procurando apenas por ali, diz ele, “é apenas o senso comum, aqui tem luz.” Em menor escala, as opiniões sobre o assunto riscos da empresa segue a mesma trajetória. Os furacões, terremotos, fraudes de alto nível e grandes erros de contabilidade estão visíveis e, embora nem todos concordem com o caminho para mitigação desses riscos, há pelo menos consenso que, de fato, tais eventos representam os riscos mais evidentes.

Para os auditores, a luz do poste que brilha sobre os riscos altamente visíveis é o foco de seu trabalho. Agentes de destruição silenciosos, mas corrosivos, podem ter sido esquecidos porque são acrescidos e expressam-se apenas ao longo do tempo.

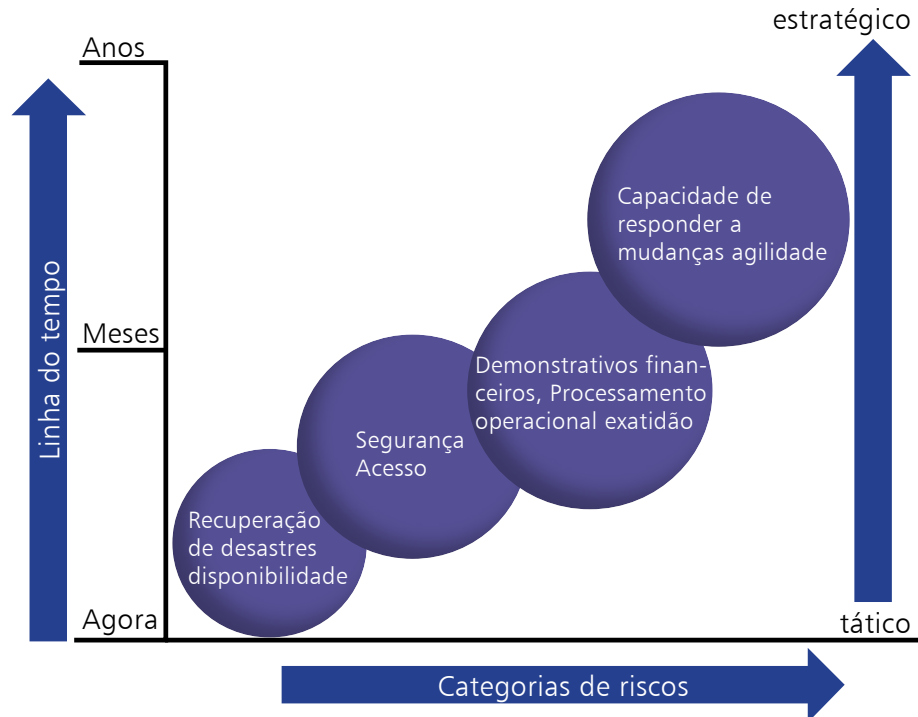
A figura 1 (ao lado) ilustra a relação geral entre as categorias de risco e os seus prazos aplicáveis. Os riscos estratégicos, que podem ou não serem maiores em magnitude do que os riscos táticos que são menos visíveis. Peter Weill e Jeanne Ross em seu livro de *TI Savvy*, apontam o efeito da curva normal, fora do padrão, quando sistemas não integrados se proliferaram:

**Muitos profissionais de TI são hábeis em fazer sistemas díspares parecerem integrados, mas o código necessário para conectar as aplicações se torna cada vez mais complexo. Com o tempo, esses sistemas têm links para muitos outros sistemas de tal forma que, mesmo as pequenas mudanças são demoradas, caras e arriscadas.**

A mesma falta de padronização mencionada anteriormente também pode ser vista sob a perspectiva de plataforma. Se uma organização compromete seu escasso capital para o desenvolvimento de capacidades específicas de TI, ela precisa ter certeza de que a base tecnológica ou de uma plataforma é estável e está bem definida.

Do mesmo modo que os construtores de uma casa precisam trabalhar com métricas de forma consistente - metros ou pés - desenvolvedores também necessitam a garantia de que as tecnologias necessárias estarão disponíveis e devidamente controladas para que eles possam contar com um conjunto mínimo de recursos. Por exemplo, suponha que uma empresa tem um único sistema ERP em toda a organização, e precisa instalar um pacote fiscal de vendas. Se o novo software exige uma interface de serviço web, todas as aplicações relevantes podem ser ligadas ao pacote usando a mesma interface. Em contraste, para uma organização com vários pequenos sistemas ERP, a instalação do mesmo pacote vai exigir um esforço muito maior,

Figura 01 | Visibilidade do Riscos vs a linha do tempo



desde que múltiplas interfaces serão necessárias. Além disso, o risco do erro no calculo de um imposto sobre as vendas aumenta com o número de interfaces originais exigidas.

Se os auditores de TI olharem para além das três categorias de risco (disponibilidade, acesso e precisão) e passarem para o domínio da estratégia (agilidade), a próxima pergunta é: Como? As áreas de risco tradicionais, tais como recuperação de desastres e continuidade de negócios, já são consideradas dentro do escopo das revisões e planejamento de auditoria. Visar na estratégia não é comum. No entanto, esta visão é sugerida para a auditoria como uma orientação de alto retorno para a empresa. A seguir estão descritas as possíveis formas de se introduzir a categoria de risco "agilidade" na carteira tradicional de avaliação de riscos de TI.

## A FUNÇÃO DO AUDITOR QUANDO AVALIA O RISCO DA INÉRCIA

Como os auditores podem fazer uso desses conceitos no seu dia-a-dia? São preocupações estratégicas apenas da

competência da direção, ou eles têm um lugar na avaliação dos auditores de risco? No passado, talvez não, mas no século 21, a sobrevivência organizacional depende de sua agilidade. A sua importância exige que essa categoria de risco seja incluída em qualquer análise significativa de risco.

Infelizmente, não há “receita de bolo” nem “produtos enlatados” para a auditora efetuar a análise do risco da inércia. Certamente, há guias funcionais de TI, apontando para a presença ou ausência de flexibilidade de sistemas, e até conjuntos adequados de ferramentas e estruturas de informação. Mas apenas isso. Os 2 itens abaixo apresentam exemplos de características das organizações com o risco inércia baixo (desejável) e risco inércia elevado (indesejável). Essas características são apenas algumas poucas sugestões. As organizações da vida real variam tanto que uma simples lista de verificação da “agilidade” não seria viável ou prática.

Características de empresas com risco de TI baixo na categoria Inércia

- Novos produtos, processos, locais geográficos e aquisições diversas podem ser incorporados facilmente à empresa sem custos excessivos, tempo ou indisponibilidade dos serviços no resto da empresa ou em TI.
- Sistemas podem ser escalados ou implementados em outras unidades de negócio, com baixo risco de indisponibilidade de serviços.
- Unidades de negócio podem ser comercializadas sem a necessidade de se considerar todos os custos de desmembramento.
- Todos os sistemas são padronizados (protocolos, plataformas

banco de dados, middleware, etc), permitindo que novas aplicações possam ser facilmente integradas às plataformas existentes.

- Ferramentas de desenvolvimento, tecnologias de banco de dados, linguagens e componentes de TI estão sempre atualizados, de forma que podem passar sem traumas por um processo de outsourcing.
- A empresa faz uso de SaaS (Software as a Service) para externar aplicações. Por exemplo, se empresa simplesmente necessita pagar seus funcionários, faz uso de um sistema de folha de pagamentos hospedado num provedor externo, pagando pelo serviço quando necessário, sem a necessidade de manter recursos especificamente para este fim.
- Arquitetura que prioriza a reutilização de software, algoritmos e processos permite a criação rápida de sistemas que atendam as necessidades de negócio. SOA (*Service-oriented architecture*) se encaixa perfeitamente nesse modelo. Até mesmo uma implementação parcial do SOA já acelera a entrega e o compartilhamento de componentes de processamento.





- O modelo de negócio é usado como base para sistemas de TI uniformes. No caso de um banco, por exemplo, existem processos padronizados para a abertura de contas, análise de crédito, gerenciamento de relação entre produtos etc. O modelo é traduzido para sistemas específicos de TI que se tornam uniformes através de toda a empresa.
- Toda a infraestrutura é padronizada, documentada e arquitetada de forma a suportar as aplicações de negócio.
- Os dados não estruturados (vitais para desenvolvimentos rápidos) estão disponíveis em locais seguros dentro da arquitetura de TI. Por exemplo, não são deixados isolados dentro de discos rígidos individuais, sem controles de acesso.
- Sistemas de TI têm a capacidade de atender aos imprevistos do cliente em função da demanda do negócio, em vez de meramente atender seus pedidos planejados. Existe uma fábrica de software conectada aos sistemas de TI, flexível o suficiente para atender rapidamente as necessidades do cliente.
- O kit de ferramentas de TI na área de desenvolvimento pode atender requisitos de virtualização, computação nas nuvens, fluxo de informação e outras transações demandadas por negócio.

Características de empresas com risco de TI alto na categoria Inércia

- Sistemas não são escaláveis e não comportam crescimentos. O sistema de reclamação do processo

de garantia foi escrito em Microsoft Access, para processar 50 reclamações por semana e agora tem de suportar 100 reclamações por dia, porque o negócio prosperou ou porque o produto ou serviço comercializado apresenta defeito de fabricação.

- As conexões entre as filiais e a matriz estão mal projetadas e não são padronizadas. Separar os sistemas das filiais e da matriz pode ter custos inviáveis influenciando até nos processos decisórios de negócio.



- Sistemas desenvolvidos sem considerar o modelo de negócio da empresa. Provavelmente uma aquisição de software, hardware, plataforma, banco de dados etc é uma roleta russa em termos de custos e riscos para o negócio.
- O software de um fornecedor é modificado descentralizadamente por cada uma das unidades de negócio dentro da empresa. Como resultado prolifera códigos customizados mais do que o necessário,

aumentando o tempo, custos e o risco quando for necessário realizar uma mudança corporativa ou da introdução de uma nova versão do código executável.

Os sistemas de ERP estão varias versões desatualizadas, impossibilitando a instalação de *add-ins* novos, aumentando sobremaneira os custos e tempo de desenvolvimento.

- Existe uma visão pobre sobre o inventário, ordens de compra e de venda, etc através da empresa por conta do processamento pesado que tem de ser executado para padronizar os dados que existem em formatos dispares.

O aplicativo de *workflow* foi desenvolvido *hard coded*. É impossível adicionar novos processos sem ter de reescrever o aplicativo e testá-lo extensivamente.

Audidores executam, tipicamente, avaliações formais de risco para ajudar a manter os planos anuais de auditoria. A fraqueza de muitas das avaliações de risco é sua dependência de um modelo simplificado ou uma perspectiva estreita. Por exemplo, é improvável que uma análise de risco de 2000 ameaças à lucratividade da Enciclopédia Britannica teria considerado o impacto negativo das vendas sobre os artigos gerados por usuários encontrados na Wikipédia.

A chave para a contenção do risco não é a capacidade de prever riscos específicos, mas a agilidade para responder a eventos imprevisíveis, desastres físicos, mudanças tecnológicas ou simplesmente as inconstantes mudanças no gosto dos consumidores.

Para equipes de auditoria tentando incluir preocupações mais estratégicas na sua avaliação de riscos, incluindo o risco da falta de agilidade num processo, pode ser

começar com projetos específicos. Ao invés de abordar toda a empresa sobre o risco da falta de agilidade, tudo de uma vez, que tal começar analisando o grau de “agilidade” para um novo sistema em desenvolvimento? Pode ser um ponto de entrada mais fácil. Por exemplo, se um pacote fora do padrão é proposto como solução, o auditor pode fazer perguntas tais como:

Como os dados serão integrados com o resto da organização?

Que rotinas de interface terão de ser escritas?

Este pacote pode ser facilmente modificado de acordo com as mudanças do modelo de negócio?

A segurança deste pacote pode ser integrada ao sistema de segurança existente(s), ou necessitará um diretório separado de segurança para ser mantido?

Por exemplo, pode se fazer uso do pacote Windows Active Directory, ou é necessário um em separado, ou o diretório do usuário deve ser mantido duplicado?



## CONCLUSÃO

Na vida das organizações de grande porte, muitos fatores importantes não podem ser quantificados ou podem ser quantificados apenas por um simples termo “sim / não” ou “grande / médio / pequeno”. Isso não significa que tais fatores não são importantes. Por exemplo, a moral, o entusiasmo com o trabalho e o grau de flexibilidade do trabalho afeta fortemente o desempenho da empresa, mas são difíceis de medir.

A agilidade cai no mesmo campo. É uma categoria de risco que pode parecer confusa, mas é importante considerar nos dias de hoje. Os auditores devem pensar

em incluir a categoria de risco “Agilidade” no seu kit de ferramentas de avaliação.

O ritmo das mudanças nos negócios e na sociedade exige que as organizações mantenham sistemas de TI que sejam ágeis. É fundamental para a capacidade de mudar rapidamente produtos e serviços, alienação e aquisição de subsidiárias, sem esforço excessivo, somado aos sistemas de escala para cima e para baixo, e a ligação de novos elementos de computação social. O auditor deve incluir uma avaliação da inércia como parte de uma revisão estratégica de riscos de TI.

Só os paranoicos e os ágeis sobrevivem.

**André Pitkowski**

Consultor na área de Governança, Risco e Compliance.

sumário





# OS DESAFIOS DEPEDEM DE VOCÊ!!!

## Especialização

Gestão de Riscos e Segurança Empresarial

Gestão de Riscos e Fraudes Empresariais

## Extensão Universitária

ISO 31000

Plano de Continuidade de Negócios

Auditoria Baseada em Riscos

Análise de Risco Estratégica

Fraudes Empresariais

## Ensino a Distância

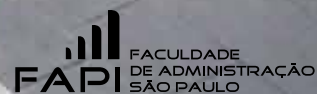
MBS - Avançado de Segurança Empresarial

Segurança Eletrônica



informações | 11 5531-6171  
| [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)

convênio:





# Gerenciando o Superior Hierárquico

Nino Ricardo Meireles

Gerenciar o superior hierárquico envolve uma abordagem consciente de seu relacionamento funcional com ele, objetivando atingir metas acordadas que beneficiarão a ambos e à empresa.

Quando se consegue gerenciar o superior, o processo inteiro de gestão se torna mais fácil, pois estarão sendo utilizadas todas as experiências e recursos de ambos para a solução de problemas, em vez de, simplesmente, falar sobre eles, ignorá-los ou acobertá-los.

Quando o gestor desenvolve uma forte relação com seu superior, isso pode aumentar sua eficácia e facilitar sua vida profissional. Se o gestor não desenvolver uma forte relação com seu superior, qualquer desentendimento ou falta de comunicação poderá desviar a atenção que deveria ser dirigida ao cliente e à concorrência. Veja abaixo o que ocorre se essa relação for negligenciada:

- As metas e prioridades do gestor podem estar opostas às do superior, o que poderá levar à frustração e/ou insatisfação de um ou ambos.
- A comunicação entre o gestor e o superior poderá tornar-se ineficaz ou até mesmo inexistente.
- A avaliação do desempenho do gestor poderá ser afetada.
- O superior poderá se sentir forçado a agir no lugar do gestor, liderando as pessoas que deveriam se reportar ao gestor.

## DESENVOLVENDO UM RELACIONAMENTO COM O SUPERIOR

É prudente que o gestor assuma a responsabilidade primária de moldar seu relacionamento com o superior. É importante que o superior perceba o valor que o gestor dá ao relacionamento entre eles. As seguintes diretrizes podem ajudar a construir um relacionamento produtivo:

- Considerar o relacionamento como uma parceria.
- Estabelecer um acordo no que diz respeito às expectativas mútuas.
- Pedir ao superior que compartilhe as metas.
- Deixar claro ao superior o que o gestor pode fazer por ele.

- Ao dar informações, o gestor deve preocupar-se com o estilo a ser utilizado.
- Produzir os resultados esperados pelo superior.
- Usar sabiamente o tempo do superior.

Para desenvolver um relacionamento com o superior, o gestor deverá ser capaz de ver o mundo através dos olhos dele, ou seja, deve desenvolver a empatia. Além disso, deve buscar conhecer a si próprio.

O gestor deverá comunicar-se com o superior de uma forma que seja adequada ao estilo dele. Com base nessa premissa, devem ser observados alguns pontos:

- Determinar se o superior gosta mais de ouvir ou de ler.
- Determinar se o superior prefere receber fatos e números bem detalhados ou apenas um esboço.
- Determinar a frequência com a qual o superior quer receber as informações.

É através da habilidade de ouvir que o gestor conseguirá obter o máximo das interações regulares com o superior. É importante tentar ser um bom ouvinte. Enquanto ouvir, tentar identificar as mensagens por detrás das palavras.

Muitas pessoas hesitam em discordar de seus superiores. Acham que serão vistos como negativistas ou que, por agirem assim, estimularão uma reação defensiva. A questão-chave é discordar de maneira construtiva, procedendo da seguinte maneira:

- Fazer com que as idéias ou o feedback estejam alinhados com as metas da empresa e do superior.
- Apresentar sugestões, em vez de apenas objeções.
- Explicar como as idéias poderão ajudar a evitar problemas em potencial.
- Dar opções.

Quando for negociar prioridades com o superior, o gestor deverá equilibrar o entendimento de ambos sobre o trabalho e seus resultados, seguindo os pontos abaixo:

- O gestor deverá deixar bem claro que está consciente da importância de todos os projetos.
- Ao determinar os prazos para novos projetos, o gestor deve pedir ajuda ao superior para evitar impactos negativos nos outros projetos.

Para desenvolver um relacionamento com o superior existem alguns passos que devem ser seguidos pelo gestor:

- Compreender tanto o seu estilo e perspectivas quanto os do seu superior.
- Determinar como ele e o superior vão trabalhar.
- Buscar um acordo no que diz respeito a metas e expectativas.
- Rever suas metas e os processos de interação e, se for necessário, mudá-los.

Para apresentar problemas ou oportunidades ao superior, o gestor deve:

- descrever o problema ou a oportunidade;
- expor as implicações da solução ou abordagem;
- discutir os benefícios da solução ou abordagem e
- aceitar a responsabilidade pelos resultados.

Sucesso.

**Nino Ricardo Meireles**

Professor, consultor, Especialista em Gestão de Riscos Corporativos e Autor de vários livros na área de segurança empresarial.

*sumário*





## A LUCRATIVIDADE ENTRE PP E SEGURANÇA

Vivemos numa conjuntura de mercado onde as margens de lucro dos varejistas são, em geral e já a algum tempo, bem pequenas. Por isso, esses agentes econômicos priorizam operações que possam gerar eficiência, com o objetivo de reduzir despesas.

A melhor maneira desta, que constitui a maior fatia do comércio, reduzir suas despesas é com a gestão de processos, pessoas e produtos, buscando a identificação das causas que influenciam diretamente na redução dos lucros.

A preocupação com perdas - lucro ou resultado não alcançado por motivo de extravio, desperdício, quebra ou administração ineficiente - é indispensável para o sucesso empresarial.

Gestão das perdas, ou seja, o meio utilizado para minimizar a probabilidade de concretização das perdas, e o gerenciamento pelas diretrizes potencializam o crescimento das empresas para que estas superem seus concorrentes e atendam às exigências do mercado.

Nesse âmbito, a segurança empresarial aparece como maior aliada dos gestores na prevenção de perdas da corporação.



“O sistema preventivo e contingencial de segurança serão desenvolvidos para dar suporte ao alcance das metas desenvolvidas pela alta administração, ou seja, a gestão da segurança não é uma coisa a parte, mas sim integrada ao negócio da empresa”, explica o Prof. Nino Ricardo Meireles em sua obra *Processos e Métodos em: Prevenção de Perdas e Segurança Empresarial* (Sicurezza, 2010).

Mas para que o gestor da segurança corporativa possa atuar na gestão de perdas é necessário que ele tenha conhecimentos específicos desta área da segurança empresarial.

O objetivo do livro, segundo o autor, é o de “busca dotar os gestores dos conhecimentos necessários para serem capazes de fazer uma gestão científica e alinhada com a estratégia da empresa”, e ele o faz. Em mais de 400 páginas a obra não deixa lacunas quanto aos métodos e processos necessários para uma eficiente gestão de perdas. Além disso, suplementa o tema abordando o papel fundamental da segurança para o êxito do propósito.

Confira informações sobre o lançamento do livro no Blog da Brasiliano & Associados.

## UM ESTUDO DE CENÁRIOS PARA MITIGAR RISCOS

O que fazer para saber algo acerca do futuro com base nas experiências adquiridas até o presente? Como diminuir as incertezas em relação aos riscos certos e possíveis?

Antonio Celso Ribeiro Brasileiro, em sua tese *Cenários Prospectivos em Gestão de Riscos Corporativos: estudo de caso da segurança pública e privada brasileira – Rio de Janeiro* (Sicurezza, 2010) faz da elaboração de cenários, uma maneira de “transformar a incerteza total em incerteza parcial”. Segundo o autor, “este é o objetivo do gerenciamento de riscos ao elaborar cenários prospectivos, específicos de riscos corporativos [...] pois o próprio gerenciamento de riscos é a análise de condições futuras”.

O autor explica que as organizações de uns anos para cá, vivenciando o cenário da Nova Economia, começaram a observar e sentir que as consequências em função da concretização dos riscos poderiam ser catastróficas para seus negócios. Mesmo levando em consideração que o risco acompanhe o homem e seja inerente à sua natureza, com o ganho de amplitude acelerado com a economia globalizada, os homens e suas respectivas organizações não encontram-se preparados para lidar com as possibilidades de eventos incertos que se multiplicaram.

Por isso, nota na obra que “para o efetivo gerenciamento de riscos decorrentes das atividades desenvolvidas nas organizações [...], é necessária a elaboração de cenários prospectivos para que os gestores tenham a visão holística das variáveis externas, com o estudo de suas respectivas interferências e interações.

Sobre as contribuições conferidas ao estudo de cenários, Brasileiro cita Schwartz, e diz que além da escolha de estratégias, outros tipos de contribuição podem ser considerados, tais como “a unificação da linguagem da organização, o auxílio no desenvolvimento de sua criatividade e a criação de redes de informação”.

De modo geral, dentre outros objetivos específicos, a tese visa “construir um referencial teórico metodológico de monitoração de cenários prospectivos, específico para a segurança pública e privada, que facilite a implantação e execução deste processo nas organizações, permitindo aos seus gestores uma melhor compreensão dos riscos que possam impactar os seus negócios.

Portanto, se você quer aprender a identificar as incertezas irreduzíveis, aproveitar os conhecimentos disponíveis dos colaboradores da empresa, abarcar perspectivas externas e saber moldar tudo isso à sua organização, deve aprender a construir cenários.

Antes, porém, e, sobretudo, vale ler a obra de Brasileiro, que, além de fornecer metodologia para o estudo, traz casos e mostra-se coerente ao demonstrar a própria tese e sua base de partida.

O lançamento do livro será em breve, com divulgação no Blog da B&A.





Editora Sicurezza, trazendo a informação!!

CONFIRA AS PUBLICAÇÕES DE 2010



para comprar, acesse:  
[www.sicurezzaeditora.com.br](http://www.sicurezzaeditora.com.br)

sumário

# BRASIL E ANGOLA,

AGORA JUNTOS NA GESTÃO INTEGRADA DE RISCO



Em 2008, a **Brasiliano & Associados**, através de um contrato de transferência de know-how da sua metodologia, processos e experiência abriu a **Brasiliano & Associados Angola**. A **Brasiliano & Associados Angola** é uma empresa 100% angolana, trabalhando com os mesmos padrões, moldes e processos da sua co-irmã brasileira. O objetivo é formar e qualificar consultores técnicos angolanos para estarem elaborando soluções na **Gestão de Riscos Corporativos**.

**COMPARTILHE DESTE DESAFIO!!!!**



**Sede Angola:** | Telemóvel: 244 929 529908 / 224 936 466677

| e-mail: [abrasiliano@brasiliano.com.br](mailto:abrasiliano@brasiliano.com.br) | [ayrton@brasiliano.com.br](mailto:ayrton@brasiliano.com.br)

| site: [www.brasiliano.com.br](http://www.brasiliano.com.br)