ISSN 1678-2496N

b&a BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

setembro 2009 | edição 47

ISO 31000
Novo Desafio

ESPECIAL

Gestão de Risco Positivo

ENTREVISTA

Alberto Bastos focaliza a ISO 31000

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 Brasiliano e Enza Cirelli. **Edição e Revisão** | Mariana Fernandez. **Arte e Diagramação** | BM Design

Colunistas | Álvaro Takei e Mariana Fernandez. **Colaboradores desta edição** | André Macieira e Andre Pitkowski

Brasiliano & Associados Online | www.brasiliano.com.br **Blog da Brasiliano & Associados** | www.brasiliano.com.br/blog

Iso 31000: : Visão Prospectiva do Gestor de Riscos Corporativo

A inovação é a capacidade de imaginar conceitos drasticamente diferentes ou novas maneiras completamente novas de diferenciar conceitos já existentes. Assim, a inovação é a chave para a criação da nova riqueza. A competição se desenvolve, nos tempos modernos, não mais entre produtos e empresas, mas entre modelos e conceitos.

Muito bem, isso quer dizer que os gestores de riscos, devem possuir uma visão holística, devem ter a capacidade de pensar de forma prospectiva, FORA DA CAIXA. O pensar fora da caixa obriga o gestor de riscos a enxergar coisas além do alcance comum, obriga o gestor de riscos a não dogmatizar processos e estratégias, obriga o gestor a raciocinar em termos de novos conceitos, capazes de suportar os riscos corporativos que, hoje, são de extrema dinamicidade.

A área de riscos corporativos tem de ser capaz de imaginar formas não ortodoxas, de revigorar o conceito preventivo. Esse enfoque é estratégico, pois além de mitigar condições inseguras em inúmeros processos, possui também, como alavanca, o gerenciamento de situações de contingência e a visualização das oportunidades. A ISO 31000, que está nascendo no final de outubro e início de novembro de 2009, já está com essa visão prospectiva.

A ISO 31000 oferecerá um novo padrão "internacional" de Gestão de Riscos, independentemente da área ou segmento de atuação. Fornecerá também um processo de Gestão de Riscos, processo esse que deverá fazer as empresas e os gestores de riscos quebrarem o isolamento entre as áreas, tão comum no mundo corporativo. Hoje, a gestão de riscos corporativos acaba sendo tratada de forma isolada, ocasionando muitas vezes a geração dos chamados silos ou ilhas departamentais, o que ocasiona a utilização de terminologias, sistemas, critérios e conceitos diferentes para cada uma das áreas da empresa. A ISO 31000 possui como grande desafio estabelecer uma linguagem comum, bem como padronizar as melhores práticas e abordagens para que as organizações possam implementar a gestão de riscos em seus processos. Por se tratar de uma proposta de convergência alinhada com a visão integrada de ERM (Enterprise Risk Management), a nova norma não concorre com outras orientações já existentes, apenas fornece orientações e alinhamento com outros conjuntos de regras específicos.

A ISO 31000 possui a visão de futuro que significa antecipação, conspiração com foco em mudanças ambientais visando reestruturar contextos. Como disse Sêneca, "não existe vento favorável para o homem que não sabe para onde ele está indo". Somente a antecipação aponta o caminho para a ação e dá duplamente sentido e direção.

Infelizmente para nós da área de riscos, não existem estatísticas para o futuro e as únicas ferramentas são a análise e a interpretação de cenários como forma de lidar com o desconhecido. A incerteza do futuro pode ser apreciada através do número de cenários possíveis dentro do campo dos prováveis.

A ISO 31000 vem ajudar a preencher essa lacuna!! Compre esse desafio!!!

Boas leitura e sorte!!!

Antonio Celso Ribeiro Brasiliano
Publisher
abrasiliano@brasiliano.com.br


sua EMPRESA possui TÉCNICAS para GERENCIAR riscos ?
Ou simplesmente salta para o infinito...
Para sua empresa ser COMPETITIVA, possuir FLEXIBILIDADE e AGILIDADE, há necessidade de compreender a dinâmica dos seus riscos corporativos
A Brasiliano&Associados ajuda você através de metodologia interativa, identificar, analisar e tratar os riscos e os seus fatores facilitadores. Propõe soluções integradas, com uma visão holística do contexto, otimizando recursos na mitigação e gerenciamento de riscos.
b&a
BRASILIANO&ASSOCIADOS
informações | www.brasiliano.com.br
| info@brasiliano.com.br

EDITORIAL

Em torno e por dentro da ISO 31000

A norma "guarda-chuva" da Gestão de Riscos é o tema da Gestão de Riscos deste mês. E, não poderia deixar de ser, já que no próximo mês, ocorrerá o lançamento da norma convergente, que trará benefícios valorosos às corporações nacionais e internacionais.

Há 4 anos houve a primeira reunião da International Organization for Standartization, a ISO, para a criação da 31000, baseada na norma Australiana / Neozelandesa 4360 . De lá pra cá, muitas práticas e terminologias das corporações do mundo todo foram questionadas e adotadas ou não na nova norma, formando sua estrutura.

Além da presença nas reuniões de países como Alemanha, Áustria, Austrália, Canadá, China, França, Inglaterra, Itália, Japão, Suíça, Suécia, Singapura, Tailândia e Nova Zelândia, muitos comentários também, foram enviados por outros países tornando a norma o mais democrática e aplicável possível.

Somente no Brasil, contribuíram com o documento, entre tantas outras corporações, empresas como ABNT - Associação Brasileira de Normas Técnicas, ASSESPRO - Associação Brasileira das Empresas de TI, Banco do Brasil, Bayer, BNDES, CEF, CEMIG, CPQD, CQSI, EMBRAER, FEBRABAN, Martins de Almeida Advogados, Modulo Security, Petrobras, QSP, Samarco Mineração e Tribunal de Contas da União.

Mas por que foi criada uma norma exclusiva para a Gestão de Riscos? Que necessidades gerais resultaram num consenso de criação da norma ISO, uma norma internacional?

Entrevistas, artigos técnicos, mídia, treinamento: por vários ângulos, destrinchamos a nova norma. Antonio Celso Ribeiro Brasiliano relata o histórico da 31000 e traz seu *framework*, em dois artigos indispensáveis para o conhecimento do regulamento.

Na seção B&A Entrevista, Alberto Bastos, representante do Brasil junto à ISO internacional no grupo de representantes dos países que estão definindo a nova ISO de Gestão de Riscos e coordenador da Comissão Especial de Estudos em Gestão de Riscos da ABNT, não deixa que restem mais dúvidas acerca da ISO 31000. O CEO da Módulo nos fala dos desafios e promessas da nova norma, além de contar sobre os vários processos que envolveram sua criação, como as dificuldades na comunicação e tradução entre os vários comitês internacionais envolvidos na formulação do regulamento.

Mas, como se não bastasse, a GR deste mês não para por aí, trazendo mais artigos inéditos. André Macieira fala, nesta edição, sobre risco positivo. Isso mesmo, risco positivo! Porque nem sempre a Gestão de Riscos trata de possibilidades negativas.

Inagurando sua coluna de TI nesta publicação, o especialista em GR Andre Pitkowski fala da importância das pessoas no processo de gestão de riscos e da importância das soluções serem feitas para elas.

E para se instruir ainda mais a respeito da norma essencial para a Gestão de Riscos atual, Álvaro Takei traça estrutura e objetivos do curso *A nova ISO 31000: seus principais elementos*, da Brasiliano & Associados.

Boa leitura a todos, este mês, de muito boas notícias!

Mariana Fernandez
Editora

b&a
BRASILIANO & ASSOCIADOS

ISO 31000: contexto e estrutura

*Antonio Celso Ribeiro Brasiliano**

I. CONTEXTO

Durante os anos de 2007 e 2008, uma série de questões de riscos - desde a crise de liquidez nos mercados financeiros até as preocupações emergentes sobre terrorismo, clima, disponibilidade de alimentos, infra-estrutura e energia - focou a atenção global na fragilidade sistêmica dos processos estratégicos das nações e, consequentemente, do mundo.

Uma conscientização do risco e gerenciamento de risco é cada vez mais vista como um pré-requisito para o controle efetivo, tanto no setor privado como público.

Dentro desse contexto, é que, neste segundo semestre de 2009, será lançada oficialmente a ISO 31000, que possui como desafio integrar os diferentes conceitos da Gestão de Riscos Corporativos. A norma está sendo desenvolvida por uma comissão especial da ISO *(International Organization for Standardization)* e teve sua numeração definida como ISO 31000.

A ISO 31000 surgiu da necessidade de harmonizar padrões, regulamentações e frameworks publicados anteriormente e que de alguma forma estão relacionados com a gestão de riscos.

A origem da norma, que pode ser aplicada por empresas ou indivíduos e fornece diretrizes para implementação de gestão de riscos em organizações de qualquer tipo, tamanho ou área de atuação, vem da necessidade das corporações de lidar com as incertezas que podem afetar os seus objetivos.

Esses objetivos podem estar relacionados com várias atividades da organização, desde as iniciativas estratégicas como as atividades operacionais, processos ou projetos. Assim, a norma pode ser aplicada aos vários tipos de riscos ligados aos diferentes setores da organização, tais como financeiro, saúde e meio ambiente, tecnologia da informação, segurança empresarial, seguros, de projetos, entre outros, incluindo a visão moderna de que risco também é oportunidade.

A ISO 31000 surge também para integrar as diversas metodologias e terminologias, pois hoje ainda falta um consenso em relação à terminologia e aos conceitos utilizados para a gestão de riscos.

O resultado mais comum dessa equação é que a gestão de riscos acaba sendo tratada de forma isolada, fazendo com que vários gestores (saúde, meio ambiente, segurança de TI e empresarial, legal, financeiro, seguros, entre outros) trabalhem em ilhas departamentais, o que ocasiona a utilização de terminologias, sistemas, critérios e conceitos diferentes para cada uma das áreas da empresa. Ou seja, cada departamento não possui o denominado impacto cruzado, não enxerga o impacto do risco que está estudando em outras áreas e ou processos.

A ISO 31000 possui um processo consistente e uma estrutura abrangente para ajudar a assegurar um gerenciamento de risco de forma eficaz, eficiente e coerente.

Por esta razão, a abordagem é genérica fornecendo os princípios e diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto.

Segundo o texto do Projeto ABNT/CEE-63 Projeto 63.000.01-001 de agosto de 2009, elaborado pela Comissão de Estudo Especial de Gestão de Riscos da ABNT, previsto para ser equivalente à ISO 31000, em suas páginas 04 e 05, as possibilidades da gestão de riscos nas empresas são:

- aumentar a probabilidade de atingir os objetivos;
- encorajar uma gestão proativa;
- estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;
- melhorar a identificação de oportunidades e ameaças;
- atender às normas internacionais, requisitos e regulamentos pertinentes;
- melhorar o reporte das informações financeiras;
- melhorar a governança;
- melhorar a confiança das partes interessadas;
- estabelecer uma base confiável para a tomada de decisão e o planejamento;
- melhorar os controles;
- alocar e utilizar eficazmente os recursos para o tratamento dos riscos;
- melhorar a eficácia e a eficiência operacional;
- melhorar o desempenho em saúde e segurança, bem como na proteção do meio ambiente;
- melhorar a prevenção de perdas e a gestão de incidentes;
- minimizar perdas;
- melhorar a aprendizagem organizacional; e
- aumentar a resilência da organização.

2 ORGANIZAÇÃO DA NORMA

2.1 Organização

A norma possui a seguinte organização:

Introdução

1. Escopo;
2. Termos e Definições
3. Princípios
4. Estrutura
5. Processo
6. Anexos: A Atributos de uma gestão de riscos avançada

2.2 Estrutura

O sucesso da gestão de riscos depende da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda a organização, em todos os níveis. A estrutura descreve os componentes necessários do esqueleto para gerenciar riscos e a forma como eles se inter-relacionam.

O diagrama ao lado (figura 1) foi retirado do Projeto ABNT/CEE-63 Projeto 63.000.01-001 de agosto de 2009, elaborado pela Comissão de Estudo Especial de Gestão de Riscos da ABNT, previsto para ser equivalente à ISO 31000, página 15:

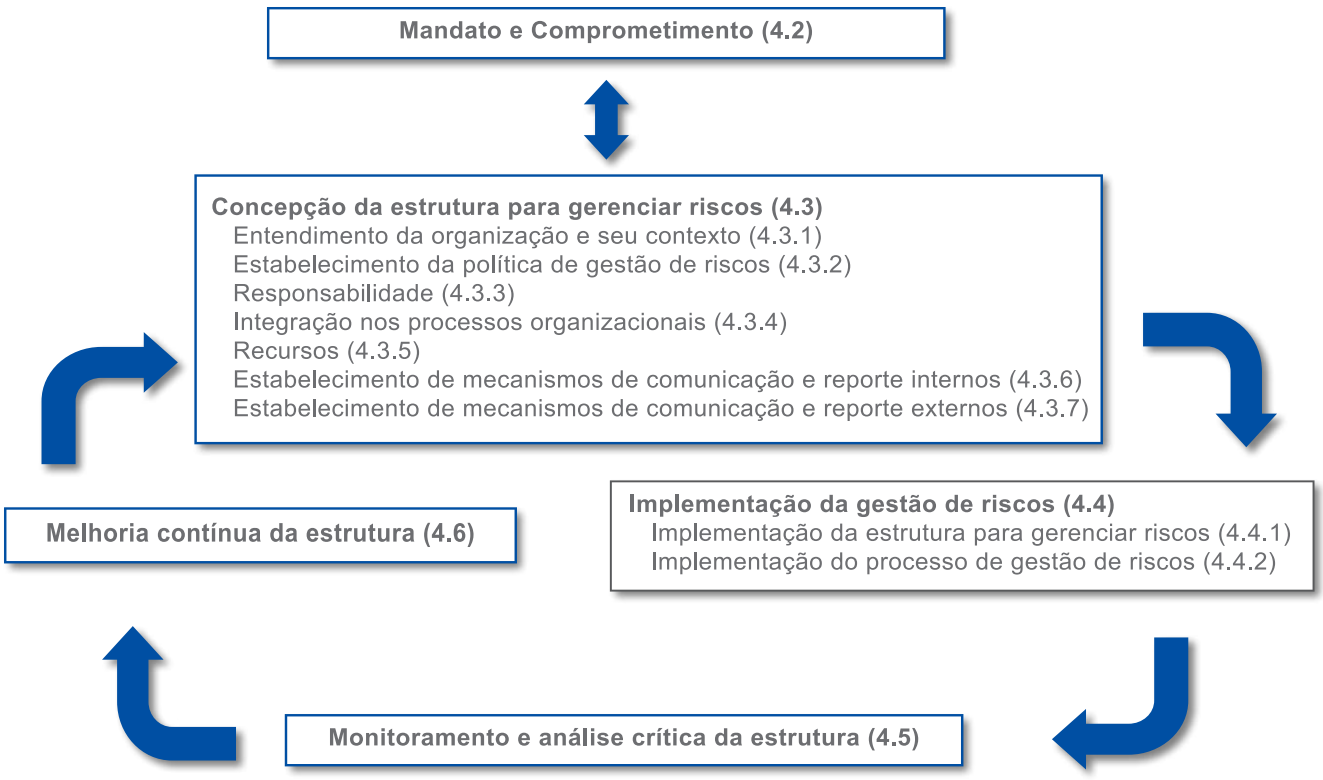


Figura 1

2.3 Processo

O processo descrito no Projeto ABNT/CEE-63 Projeto 63.000.01-001 de agosto de 2009, elaborado pela Comissão de Estudo Especial de Gestão de Riscos da ABNT, previsto para ser equivalente à ISO 31000, página 20 e 21 é:

Convém que o processo de gestão de riscos seja:

- parte integrante da gestão;

- incorporado na cultura e nas práticas, e

- adaptado aos processos de negócio da organização.

Ele compreende as seguintes atividades (Figura 2, abaixo):

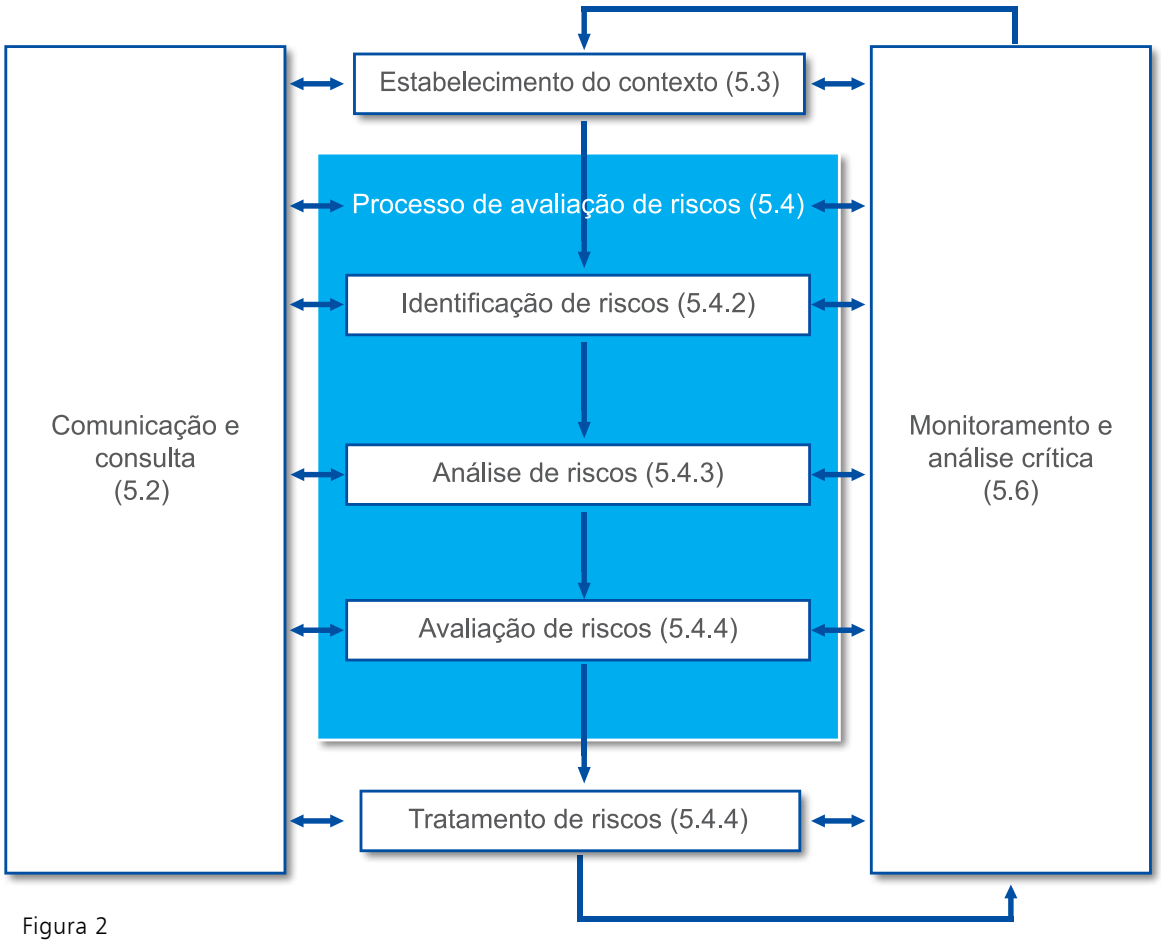


Figura 2

Genericamente o processo estruturado sugerido possui sete fases claramente identificadas, sendo um processo retroalimentativo. Ou seja, segue os princípios do ciclo da qualidade, PDCA – Plan – Do – Check – Action.

A fase de comunicação e consulta abrange todas elas e é inter-relacionada. Abrange tanto a comunicação interna quanto a externa, assegurando que os responsáveis e partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as respectivas razões.

A fase do estabelecimento do contexto preconiza entender os fatores e as variáveis externas, incluindo os fatores-chave, as tendências e as relações com as partes interessadas externas e suas percepções de valores. Já no contexto interno procura-se entender: objetivos estratégicos, cultura, processos, estrutura e estratégia. No contexto, estabelece-se o processo de gestão de riscos com sua estrutura, seus critérios e métodos que a organização deverá utilizar. Define-se metas e objetivos além de responsabilidades e o apetite ao risco que a organização quer possuir.

A fase da identificação de riscos, no processo de avaliação de riscos, é a listagem dos perigos que o processo, departamento e ou empresa possui com as respectivas fontes de riscos. A identificação deve ser crítica, pois um risco que não é identificado nesta fase não será incluído em análises posteriores. Fica claro que essa é a fase estratégica pois é nela que se entende os fatores de riscos, os fatores facilitadores da existência do risco na empresa.

A fase de análise de riscos desenvolve a compreensão dos riscos. Com a compreensão dos riscos é que a empresa poderá tomar decisões a respeito de seu tratamento. Nessa fase, estima-se a probabilidade e consequência do risco na empresa.

A análise envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. A norma não especifica critérios e métodos, pois organização é a responsável pela escolha, a qual deve respeitar as características do negócio.

A fase da avaliação de riscos visa auxiliar na tomada de decisões - com base nos resultados da análise de riscos -, sobre quais riscos necessitam de tratamento, bem como sobre qual a prioridade para a implementação do mesmo. Na avaliação de riscos, que, envolve comparar o nível de risco encontrado durante a análise de riscos, deve-se utilizar uma Matriz de Riscos como ferramenta de gestão.

A fase de Tratamento de Riscos envolve um processo cíclico composto por:

- avaliação do tratamento já realizado;
- decisão se os níveis de risco residual são toleráveis;
- se não forem toleráveis, a definição e implementação de um novo tratamento;
- avaliação e eficácia desse tratamento.

As opções de tratamento são as universais:

- ação de evitar o risco;
- tomada ou aumento do risco – se o risco for positivo;
- remoção da fonte de riscos;
- alteração da probabilidade;
- alteração das conseqüências;
- compartilhamento do risco; e
- retenção do risco por uma decisão consistente e bem embasada.

A última fase, monitoramento e análise crítica é a fase da checagem ou das vigilâncias regulares. Podem ser regulares – periódicas ou acontecerem em resposta a um fato específico. Deve haver uma definição clara e direta das responsabilidades de quem vai realizar o monitoramento e a análise crítica.

2.4 Registros do Processo de Gestão de Riscos

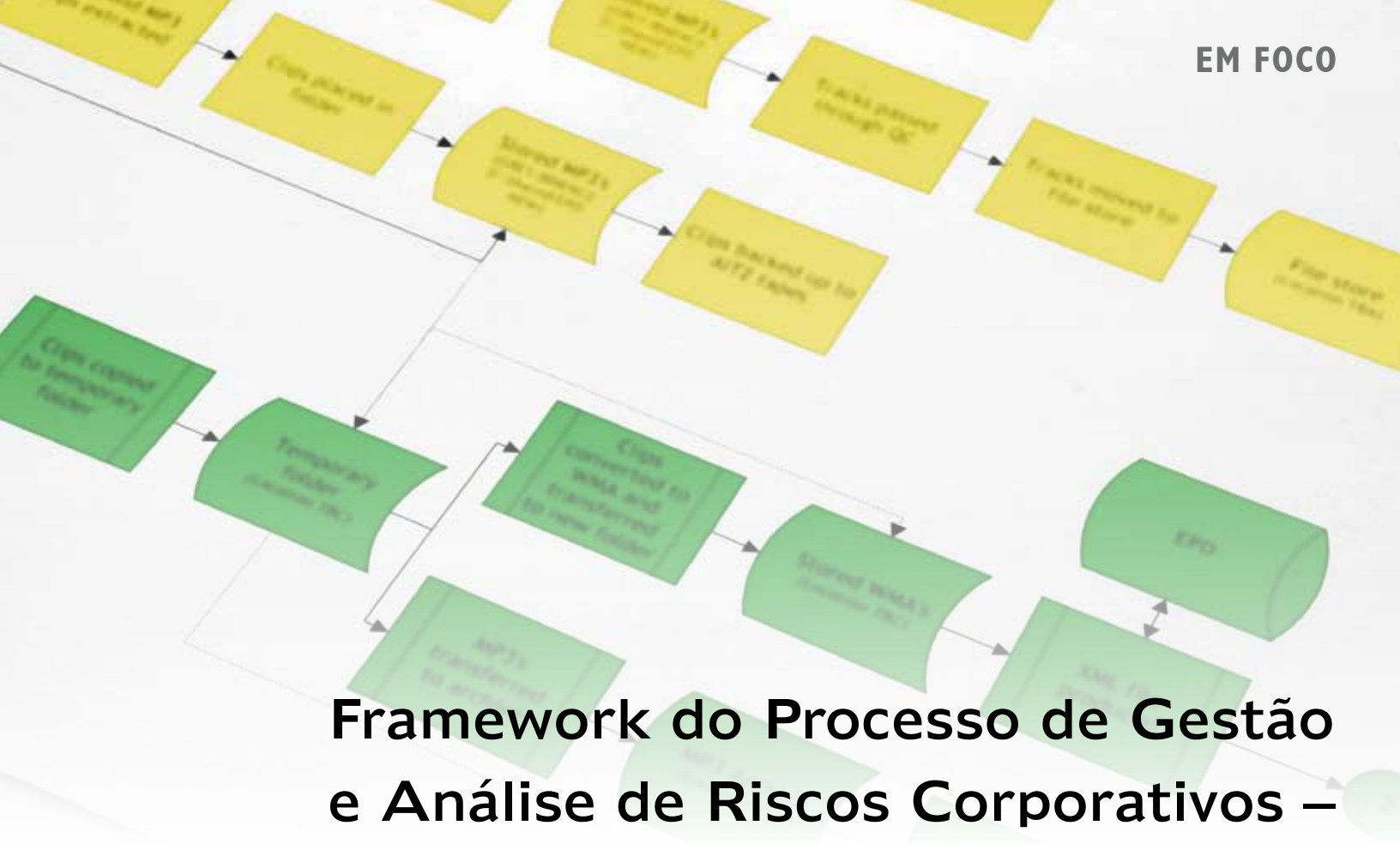
As atividades de gestão de riscos devem ser rastreáveis. Ou seja, deve haver registros, pois esses fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.

3. CONCLUSÃO

O grande desafio no desenvolvimento da ISO 31000 estava em estabelecer uma linguagem comum, bem como em padronizar as melhores práticas e abordagens para que as organizações pudessem implementar a gestão de riscos em seus processos.

Por se tratar de uma proposta de convergência alinhada com a visão integrada de ERM (Enterprise Risk Management), a nova norma não concorre com outras orientações já existentes, fornecendo orientações e alinhamento com outros conjuntos de regras específicos.

Antonio Celso Ribeiro Brasiliano
Publisher da Revista Gestão de Risco
e Diretor da Brasiliano & Associados
abrasiliano@brasiliano.com.br



Framework do Processo de Gestão e Análise de Riscos Corporativos – Método Brasiliano Avançado

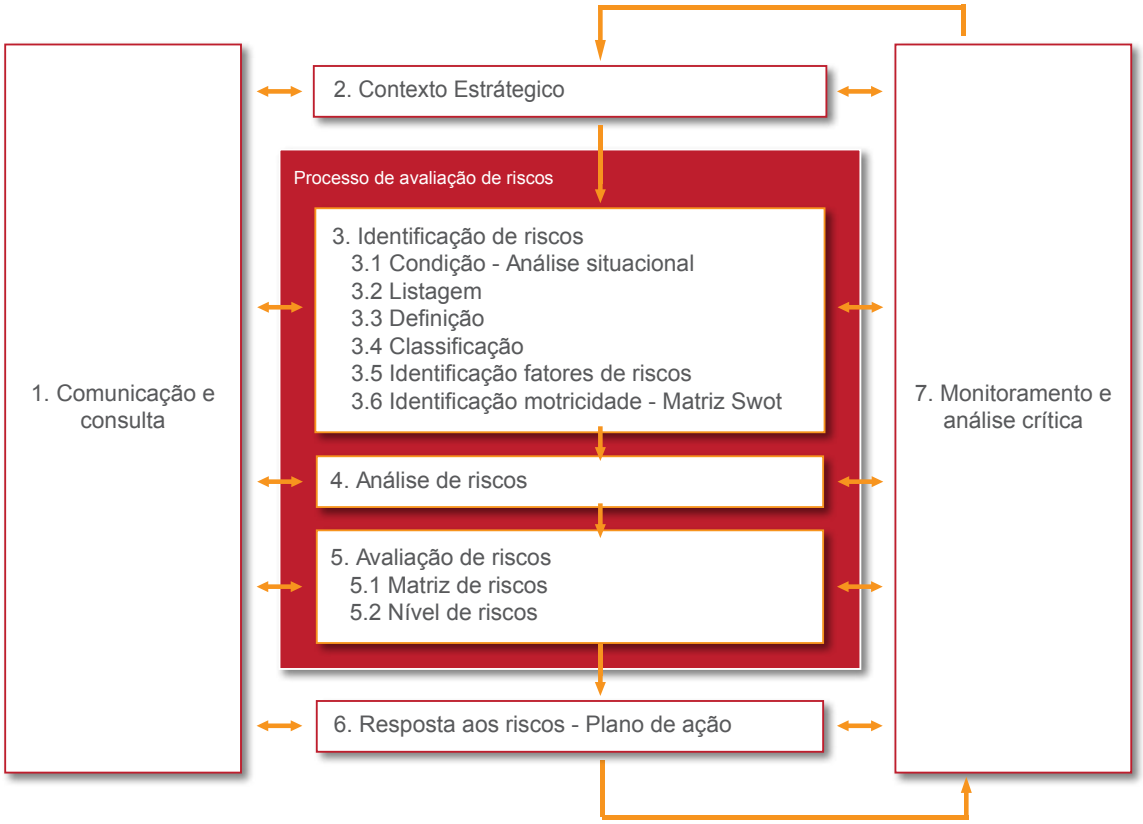
*Antonio Celso Ribeiro Brasiliano**

I. VISÃO GERAL DO MÉTODO

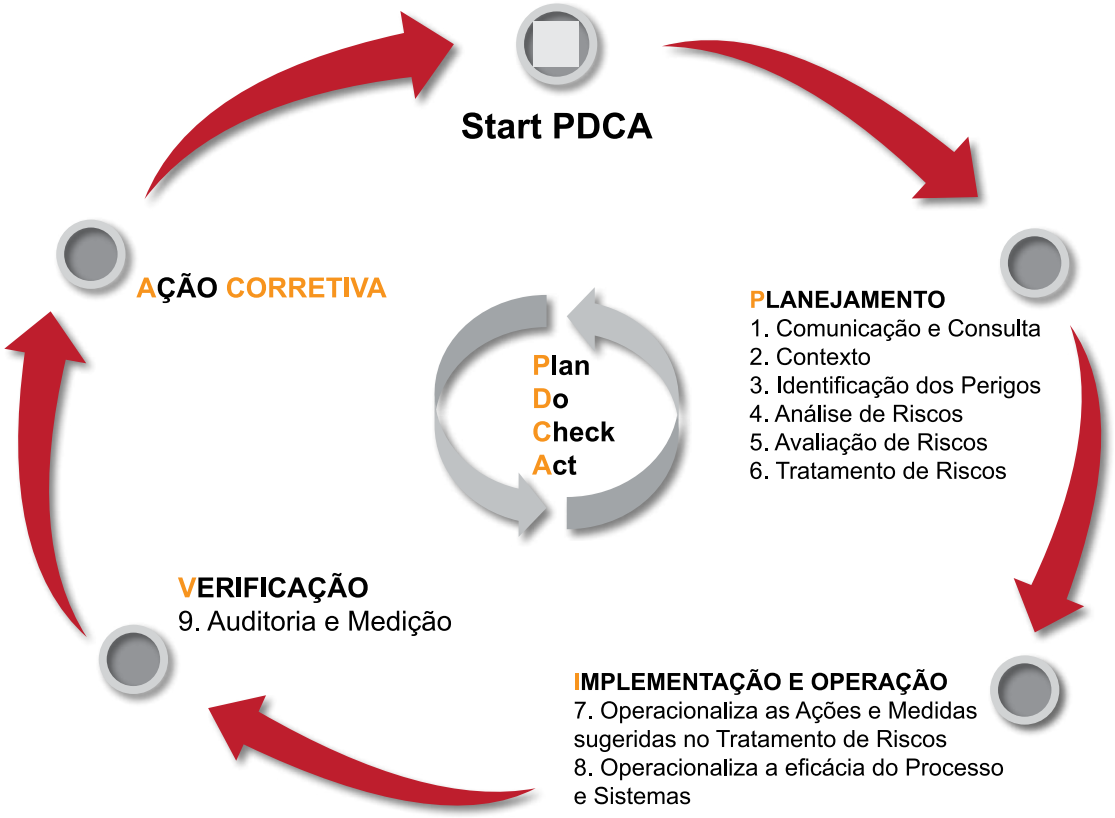
O gerenciamento do risco é uma parte do processo de gerenciamento empresarial. É um processo de múltiplas facetas, aspectos adequados dos quais são frequentemente melhores realizados por uma equipe multidisciplinar. É um processo interativo de melhoria contínua.

O Método Avançado de Gestão e Análise de Riscos Corporativos – Método Brasiliano possui como elementos principais do processo o mostrado na figura abaixo, os quais estão alinhados com a Futura Norma ISO 31000. Os elementos principais do processo estão integrados no ciclo do P (Plan) D (Do) C (Check) A (Action).

No Método Brasiliano sugerimos ferramentas e critérios nas fases de identificação, análise e avaliação de riscos. Essas ferramentas e critérios são frutos da experiência da Brasiliano & Associados na implantação de projetos de Gestão de Riscos nas empresas clientes.



Fases do Método Brasiliano – Adaptado da ISO 31000



Ciclo PDCA x Fases de Gestão e Análise de riscos do Método Brasiliano

2. DESCRIÇÃO DOS PRINCIPAIS ELEMENTOS DO MÉTODO

2.1 Comunicação e Consulta

Comunicação e consulta é a forma como serão estabelecidos o processo e a estratégia de comunicação com as partes interessadas. É uma fase extremamente estratégica que permeia todo o processo de gestão e análise de riscos, já que, sem a comunicação, não haverá processo de gestão de riscos, pois também não haverá a sensibilização dos usuários do processo.

2.2 Contextos Estratégicos

O estabelecimento do contexto é dividido em três níveis. O primeiro diz respeito ao entendimento da empresa, através da compreensão dos objetivos estratégicos, organizacionais, da cultura e como ela – empresa – pensa sobre a questão de gestão de riscos. O segundo nível tange as variáveis externas incontroláveis que poderão interferir ou expor os objetivos estratégicos da empresa. Na verdade, há a necessidade de se construir cenários de riscos estratégicos.

O terceiro nível trata da Política de Gestão de Riscos da empresa, onde será detalhada a estrutura a ser trabalhada bem como os critérios e metodologia a serem utilizados pela empresa.

2.3 Identificação dos Perigos e dos Fatores de Riscos

Esta terceira fase possui três objetivos:

1. Identificar e listar os perigos a que a empresa, unidades, processos e ou departamentos estão expostos. A listagem deve ser realizada através de reuniões do tipo BRANISTORMING, levantando tanto os perigos conhecidos como os desconhecidos. Os perigos desconhecidos são aqueles que nunca aconteceram, porém podem ocorrer, mesmo que remotamente;
2. Identificar os Fatores de Riscos. Os Fatores de Riscos, também chamados de Fatores Facilitadores e ou Fontes de Riscos, são os eventos que podem potencializar a concretização dos perigos. São variáveis controláveis e incontroláveis. Utilizamos para isso a Ferramenta de Gestão Diagrama de Causa e Efeito;
3. Avaliar os Fatores de Riscos. A avaliação dos FR é a mensuração dos respectivos fatores com o objetivo de identificar quais são os fatores de maior importância e ou motricidade. Ou seja, quais são os fatores que devem ser tratados, quais fatores interferem no contexto de riscos. Utilizamos para isso duas ferramentas de gestão: a Matriz SWOT e ou a Matriz de Impactos Cruzados.

2.4 Análise de Riscos

Nesta fase estabelecemos critérios para os dois parâmetros universais: a probabilidade e o impacto. Os critérios para os dois parâmetros são de suma importância para a elaboração do estudo de análise de riscos. O cruzamento desses dois parâmetros tem como resultado uma Matriz de Riscos.

2.5 Avaliação de Riscos – Nível de Riscos

Comparar os níveis de riscos em relação ao critério pré-estabelecido. A relevância dos riscos possui como parâmetro a Matriz de Riscos.

O resultado da matriz de riscos é o grau de criticidade, ou seja, com que priorização a empresa deve tratar cada risco frente ao seu apetite ao risco. A matriz é dividida em quadrantes e para cada quadrante há uma estratégia de tratamento e priorização. Cabe ressaltar que é nesta fase que se estabelece o Grau de Riscos dos processos estudados e ou das unidades/sites empresariais.

2.6 Respostas aos Riscos – Plano de Ação

O Plano de Ação é o tratamento dos riscos, ou seja, a resposta que a empresa terá que operacionalizar. Aceitar, reter, reduzir, transferir, explorar e ou evitar? Desenvolver e implementar um plano específico de gerenciamento, o qual inclui consideração de provimento de fundos.

O Plano de Ação é o conjunto de medidas organizacionais, sistemas técnicos de prevenção e monitoração e recursos humanos que gerenciarão os riscos. É elaborado com base nos Fatores de Riscos visando mitigar e diminuir as probabilidades dos riscos.

2.7 Monitoração e Análise Crítica

Esta fase diz respeito ao monitoramento e revisão do desempenho das ações e sistema de gerenciamento de risco e também ao procedimento referente às mudanças que possam afetá-lo.

3. CONCLUSÃO

O framework do Método Brasiliano Avançado de Análise de Riscos, diferentemente do framework precedente, além de alinhar-se à nova norma de Gestão de Riscos Corporativos, a ISO 31000, traça novos elementos.

As fases do Método Brasiliano são: **Levantamento dos perigos e diagnóstico, Identificação dos fatores facilitadores dos perigos, Matriz Swot – FOFA, Análise de Risco, Matriciamento de Riscos e Plano de Ação. Já no Método Avançado os elementos diferem um pouco, denotando uma técnica e experiência mais avançada, sendo eles:** Construção de Cenários de Riscos – Contexto, Identificação dos Perigos e dos Fatores de Riscos, Análise de Riscos, Avaliação de Riscos, Plano de Ação – Respostas aos Riscos e Monitoração e Revisão.

O framework proposto no novo método, com a adoção de novas ferramentas possibilita uma análise de riscos mais profunda e condizente com as necessidades do gestor mais experiente, que já pratica a análise de risco embasado em conhecimento técnico e colhendo resultados proveitosos.

Antonio Celso Ribeiro Brasiliano
Publisher da Revista Gestão de Risco
e Diretor da Brasiliano & Associados
abrasiliano@brasiliano.com.br

sumário

No que difere o Método Brasiliano de Análise de Riscos, publicado pela Sicurezza, em 2006, do Método Brasiliano Avançado que será publicado em novembro de 2009 além do alinhamento com a nova ISO 31000?

Nós mudamos o framework, adaptando-o para o framework da ISO 31000, ou seja, o processo macro, o processo genérico está adaptado para o da ISO 31000. Fizemos um alinhamento, incluindo comunicação e consulta e campanha de endomarketing – tem que ter uma via de dupla mão para ter essa comunicação. Incluímos também, o que obrigatoriamente todo projeto tem que ter que é o contexto estratégico, que inclui os objetivos estratégicos da empresa, que obriga-se a ter uma política de gestão de risco e também cenários prospectivos na área de risco. Isso é uma sugestão da ISO 31000 que nós aceitamos de bom grado. Incluímos na parte de identificação de risco obrigatoriamente e assumimos o processo deles como a prática de brainstorm, que foi oficializada – então a gente faz o levantamento da área de risco via brainstorm, como conceituar esses riscos e depois vamos identificar os fatores de risco através do Diagrama de Causa e Efeito. Essa, ferramenta juntamente com a Matriz SWOT, já fazia parte do primeiro livro, então não é novidade. Mas nós incluímos, agora, neste livro, mais uma ferramenta para poder verificar qual é o nível de motricidade dos Fatores de Risco que é a Matriz de Impacto Cruzado. Então é uma ferramenta nova que está à disposição para nós podermos utilizar dependendo do tipo de projeto. Como ferramenta nova nós incluímos também o Plano de Ação, para poder ter uma priorização de ações, uma ferramenta, uma matriz com três quadrantes, colocamos alguns indicadores para que o gestor possa tomar suas decisões pensando "qual ação é prioritária frente a uma relação custo x benefício". Resumindo, o diferencial do livro é que ele está alinhado com a ISO 31000, super moderno, super novo já que a norma sai agora em outubro, além disso inclui essas duas ferramentas que eu já citei e tem o processo todo alinhado, estando todo interligado e amarrado.

Qual o principal benefício na aquisição do conhecimento metodológico em GRC?

O melhor benefício é que as empresas como um todo falarão a mesma linguagem, de forma sistematizada e padronizada. O padrão da linguagem será trazido pela ISO Guide 73. Vai ter todo um vocabulário padrão e o processo será igual para todas as áreas e segmentos. A aquisição do conhecimento metodológico de qualidade torna as empresas muito mais pró-ativas, fornecendo-lhes uma visão antecipatória em vez de uma visão de bombeiro. Ou seja, a empresa passa a ser conspiradora. Michel Godet fala que tem que ser conspirador e não ter visão de bombeiro que apaga incêndio correndo atrás do prejuízo.

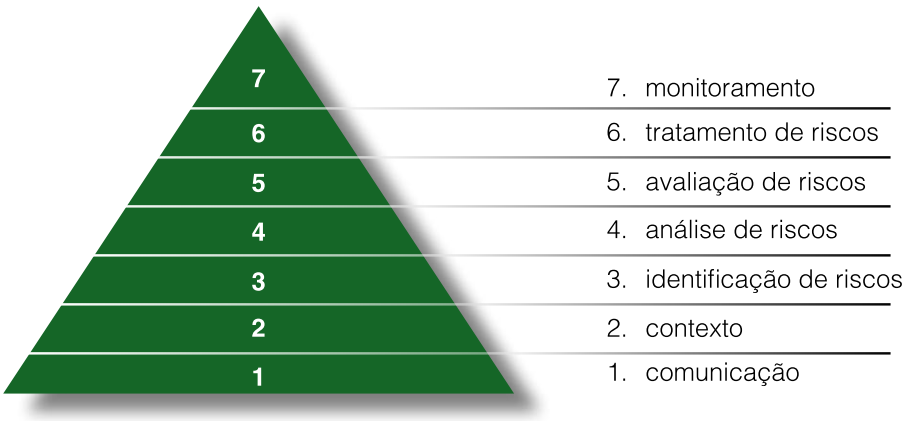
Confira a resenha completa do livro Gestão e Análise de Riscos Corporativos - Método Brasiliano Avançado na coluna Ler & Saber.

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 futura ISO 31000.



A Brasiliano pode ajudar você a elaborar seu plano de PGRC

Consulte – nos!!!!

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

Alberto Bastos focaliza a ISO 31000

Mariana Fernandez

Em entrevista à B&A, o sócio-fundador da Módulo revela o trajeto percorrido até a constituição da norma lançamento da Gestão de Riscos no mundo.

Alberto Bastos é o representante do Brasil junto à ISO internacional no grupo de representantes dos países que estão definindo a nova ISO de Gestão de Riscos. O especialista brasileiro é também o Coordenador no Brasil da Comissão Especial da ABNT sobre as normas de gestão de riscos e membro do Comitê Brasileiro sobre as normas de gestão de segurança da informação, da série 27000, que inclui a ISO/IEC 17799 e ISO/IEC 13335.

Especialista na área de Segurança da Informação, Bastos é formado em Informática pela UFRJ, com MBA Executivo pela COPPEAD/UFRJ, foi o primeiro latino-americano certificado pelo International Information Systems Security Certification Consortium como CISSP - Certified Information Systems Security Professional. É também diretor de Segurança da Informação da Assespro -RJ, membro do CSI - Computer Security Institute e da ISSA - Information Systems Security Association Inc.

Nossa entrevista ocorreu no último dia 16 em São Paulo após reunião que tratava dos últimos acertos da nova norma 31000 e de um guia de terminologias da área de gestão de risco, também da International Organization for Standartization, a ISO.

A seguir, Bastos fala da importância do Brasil como contribuinte com comentários à nova norma, especialmente no tocante a área de riscos em TI. Fala também da expectativa de adoção, dos benefícios e impactos da ISO 31000.

Como senhor se tornou o representante do Brasil na ISO na discussão das normas de gestão de risco?

Atualmente estou coordenando o Comitê de Gestão de Riscos da ABNT, e a ABNT é a associação que, aqui no Brasil, representa as normas internacionais, em específico as normas ISO que são essas normas de gestão. Então, como especialista no assunto e como coordenador do Comitê de Gestão de Riscos, eu fui indicado pra ser, vamos dizer assim, o delegado brasileiro. Na verdade, muitas vezes na delegação podem ir outras pessoas. Por duas vezes nós tivemos até a participação de pessoas da Petrobrás nas discussões e... foi assim que eu tornei o representante.

Desde quando se iniciou o processo de criação da ISO 31000?

Desde a primeira reunião que foi em Tóquio, no Japão em 2005. Depois, em 2006 foram duas reuniões uma em Sidney, na Austrália, e depois em Viena, na Áustria. Em 2007 foi em Ottawa, no Canadá e na China. Em 2008 nós só tivemos uma reunião que aconteceu em Cingapura, que foi a última. Agora em 2009 deve ocorrer uma reunião no início de outubro na Alemanha, logo após o período de fechamento e aprovação da norma, que é uma reunião simplesmente quase que editorial e a partir daí a norma tende ser publicada, provavelmente, no início de novembro ou no final de outubro.

Por que se decidiu que deveria haver uma norma específica para a gestão de riscos internacional, uma norma ISO?

Na verdade a ISO avaliou e descobriu que existiam mais de sessenta comitês técnicos ou grupos de trabalhos que desenvolviam normas em vários setores e de alguma forma estas normas diziam a respeito a gestão de riscos. Só que cada grupo desse ou cada norma, utilizava conceitos diferentes, terminologias diferentes. A partir daí houve a necessidade de se criar, principalmente dentro de um organismo de normalização, um padrão para que se padronizassem todos esses documentos, todas essas práticas. Por isso a primeira iniciativa foi criar não exatamente uma norma contendo regras mas uma norma de vocabulários e conceitos que é a ISO Guide 73, que padronizou, que criou essa linguagem comum utilizando vocabulário, terminologia e conceitos genéricos que se aplicam a todas as áreas e todos o setores. E logo em seguida, após a ISO Guide 73, que aqui no Brasil nós traduzimos e lançamos junto com a ABNT como ISO Guia 73, que é uma versão de 2002, surgiu essa iniciativa de desenvolver uma norma especifica de gestão de risco que também fosse aplicada a todas as áreas e todos os setores, uma espécie de norma guarda-chuva, uma norma orientadora para as outras normas. Daí desenrolou esse processo de criar um comitê internacional que está diretamente ligado ao TMB, o Technical Management Board, que é o conselho de gestão técnica direto da ISO. Assim criou-se um grupo de trabalho de especialistas em gestão de riscos que foi o responsável por desenvolver a ISO 31000. Nesse meio tempo a IGO Guide 73, que é uma norma de 2002, que é uma norma antiga e como padrão de quatro em quatro anos ou no máximo cinco anos uma norma é revisada, está sendo revisada juntamente com a ISO 31000. Então ambas as normas serão lançadas provavelmente agora no início de novembro simultâneamente à ISO 31000 que é uma nova norma e a nova versão da ISO Guide 73.

Porque a ISO Guide 73 tem que continuar existindo se a ISO 31000 é uma norma mais abrangente?

Uma das seções, um dos capítulos de uma norma, no caso da norma da ISO 31000 é o capítulo de terminologia e, especificamente a terminologia empregada na ISO 31000 é a própria terminologia que está definida na ISO Guide 73. Agora, existem termos e conceitos definidos na ISO Guide 73 que não estão na ISO 31000 então a proposta da ISO Guide 73 é mais abrangente que a da ISO 31000 porque abrange todos os termos e definições que foram usados na ISO 31000, mas abrange também termos e definições que são, muitas vezes, um pouco mais específicos de uma área ou de um setor mas que pra efeito de padronização, definiu-se eles na ISO Guide 73 de forma que eles pudessem ser sempre usados com a mesma palavra criando essa linguagem única.

O que foi mais difícil no processo de criação da norma?

O mais difícil foi se conseguir conciliar e chegar ao consenso diferentes áreas, diferentes termos utilizando a gestão de risco. Como a proposta da norma é ser uma norma genérica para ser utilizada em todas as áreas, em todos os setores, havia a área de seguimentos que já tinha seu modelo de gestão de risco consolidado. Então na hora que se começou a dizer que haveria a necessidade de se mudar a forma dele de pensar, há uma certa resistência a essa mudança. Para você ter uma idéia, uma das coisas mais difíceis que aconteceu nesse processo foi definir risco. Numa norma de gestão de riscos, o que é risco? Existiam várias definições mas chegou-se agora a uma definição comum, que, por consenso, atende a todas essas áreas e que de uma certa forma vai, a partir da publicação da norma, passar a ser a definição de risco amplamente aceita em todas essas áreas. A maior dificuldade sem dúvida foi esse trabalho de se discutir e de se chegar ao consenso, seja porque se tem diferentes áreas, seja porque se tem diferentes nações, porque gestão de riscos também envolve valores e crenças, então o que é um risco na China não é um risco no Japão, não é um risco no Brasil e não é um risco na Alemanha. Algumas dessas questões culturais, regulatórias... muitas vezes o risco tem a ver com a parte de conformidade com leis e regulamentos e isso varia de lugar pra lugar. Então a dificuldade foi se criar uma norma que de fato fosse abrangente, que contemplasse todas as áreas e todos os setores.

E com relação à língua também deve ter havido muita dificuldade...

É, a língua tem dificuldade mais o processo da ISO já e um pouco mais avançado nesse sentido. A ISO como principal organismo de normalização mundial desenvolve normas ISO para todas as áreas e setores como a ISO 9000 na área de qualidade, a ISO 14000 na área de meio ambiente... esse desafio da língua já é de uma certa forma o próprio processo de desenvolvimento da norma, ele já endereça de uma certa forma essa dificuldade. Mas é verdade. Uma vez o cara do Japão falava um inglês que ninguém entendia. A língua oficial é o inglês e a gente tinha, às vezes, certa dificuldade de compreender e de ser compreendido.

Acho que isso já foi falado, sobre as terminologias e os conceitos utilizados em gestão de risco que não seguiam até um momento um consenso...

É só aproveitando essa dica... alguns termos, não o conceito, o conceito é tranqüilo e todo mundo deveria entender, mas muitas vezes alguns termos utilizados, principalmente em inglês, não têm traduções fáceis no nosso português então, por conta disso, também trás alguma dificuldade. Por exemplo,

quando o americano utiliza a palavra *probability* ele está querendo dizer que é uma probabilidade científica, uma probabilidade matemática que é um número que varia de zero a um e etc. Nós aqui, quando usamos probabilidade, pode ser isso mas pode ser também alguma coisa parecida com a possibilidade. Para esse outro conceito o americano usa a palavra likelyhood, que não é uma palavra muito conhecida aqui. Então a gente tem alguns problemas de tradução, porque nós traduzimos *likelyhood* e *probability* com a mesma palavra que é probabilidade e lá eles utilizam dois conceitos diferentes para cada uma dessas palavras. Assim, nós tivemos que ter um certo trabalho ao discutir isso internamente, principalmente na hora que partirmos para traduzir essa norma para lancá-la aqui no Brasil.

Que benefícios a padronização com relação às terminologias vai trazer para as empresas, apesar da resistência delas em adotarem a norma, em mudarem suas terminologias, qual será o beneficio dessa padronização?

Muito boa pergunta... a gestão de riscos, hoje, nas organizações, é tratada de uma forma isolada. As áreas, os departamentos, as funções que de alguma forma lidam com gestão de riscos nas empresas, nas organizações também têm uma espécie de ilhas ou silos ou feudos. Então, de uma certa forma, a existência de uma norma que é uma norma genérica de gestão de risco, também ajuda a derrubar esses muros que existem entre as diferentes gestões de risco dentro da organização, fazendo uma visão mais integrada para essa gestão de risco. Hoje existe um termo, que é conhecido em inglês ERM *Enterprise Risk Management*, que a gente poderia traduzir aqui no Brasil como Gestão Integrada de Risco ou Gestão de Risco Corporativo e nessa visão integrada, essa idéia de que os riscos estão segmentados ou isolados, eles não funcionam bem, porque o risco na organização é sistêmico porque tem um efeito dómino: o risco numa área ou o risco numa pessoa que aperta outro processo que aperta outra área que aperta outra pessoa. Então acho que vai ter um grande benefício nas organizações porque elas passam a contar agora com essa linguagem comum, com essa linguagem única, que pode criar uma verdadeira revolução no sentido de fazer as áreas, as pessoas, as funções, os departamentos colaborarem mais, se integrarem mais. É um processo de convergência.

Que práticas e abordagens já adotadas pelos praticantes da gestão de riscos nas corporações foram incorporados na norma aqui no Brasil?

Praticamente todas as normas, porque o trabalho de desenvolver a norma é justamente reunir o conjunto de especialistas com as diferentes práticas e modelos de políticas de gestão e conseguir resumir o que seria o supra-sumo de todas essa melhores práticas, regras e diretrizes. Então a ISO 31000 contém as melhores práticas e as melhores diretrizes, e, um dos capítulos específicos, que é o que fala sobre a gestão de risco *enhanced*, ou avançada ou aprimorada ou turbinada, é exatamente uma gestão de risco onde estas melhores práticas são utilizadas no seu ápice. Então a norma prevê conjunto de diretrizes que são as diretrizes gerais que se aplicam praticamente em todas as empresas, sendo que em específico ela destaca algumas dessas práticas como práticas mais avançadas no nível de maturidade que seriam aplicadas em empresas que já possuem um nível de maturidade de gestão de risco, mais aprimorado.

De maneira simplificada, qual é a estrutura da norma?

A norma é muito simples. A norma basicamente tem um capítulo que fala da tecnologia, tem um capítulo que fala do framework que aqui no Brasil nós traduzimos por estrutura, que trata como

é que você vai inserir gestão de risco dentro da organização em várias áreas, em várias funções, em vários departamentos. Um capítulo que fala sobre o processo, que é exatamente essa forma de como que você, na hora em que você está inserindo a gestão de risco dentro das áreas ou funções, como é que você adapta os processos específicos; então, por exemplo, a parte de gestão de projetos que envolve gestão de riscos, hoje a área de gestão de projetos tem um processo de gestão de riscos próprio ele seria influenciado e alterado para seguir o processo da ISO 31000, a gente vai pra área de TI ou área de segurança da informação, que tem o seu processo próprio, esse processo seria influenciado e alterado segundo o processo da ISO 31000, planejamento estratégico a mesma coisa, em todas as áreas de seguro a mesma coisa: impacto, na saúde, segurança ocupacional, em todas as áreas todos os processos de uma certa forma que têm a ver com a gestão de riscos serão influenciados por esse processo que este capítulo específico. Logo em seguida seria esse anexo que seria a gestão de risco de forma avançada... na verdade eu pulei um capítulo antes do framework que são os princípios. A norma estabelece onze princípios que são os princípios gerais da gestão de riscos. A estrutura é muito simples: terminologia, princípios, estrutura e processos.

A versão brasileira da norma será lançada simultâneamente à versão em inglês?

Essa é a nossa proposta. Nós já nos mobilizamos, o documento na reunião de hoje já foi aprovado - estava em consulta nacional pela ABNT, o documento foi revisado por toda a comunidade, por toda comissão de estudo e já está praticamente aprovado – então, assim que ISO oficializar esse lançamento internacional a gente já está pronto aqui no Brasil para fazer esse lançamento quase que simultâneo.

Como é o processo e quais foram as dificuldades da tradução?

Um pouco sobre essa questão de palavras que têm uma dificuldade inerente de nós traduzirmos, pois utilizamos a mesma palavra para repetir dois conceitos. O problema muitas vezes de estilo, porque como a gente está traduzindo uma norma ISO, uma norma internacional, a gente tem que ser o mais fiel possível ao sentido dessa norma. Então, muitas vezes por uma questão de estilo, a forma de escrever do inglês, usando muito gerúndio, não é uma forma muito boa no Brasil. Então a gente tenta, de uma certa forma, contemplar essa questão de estilo. Como temos um conjunto de especialistas na comissão que são bastante experientes nesse assunto, conseguimos ter um resultado muito positivo.

Sendo uma norma convergente quais são as principais normas que se alinham à ISO 31000?

Praticamente todas essas normas desses sessenta grupos da própria ISO, mas fora da ISO também, todas essas normas vão ser impactadas. Eu coincidentemente, ontem, participei de um comitê técnico da ABNT, o CD21, que é o comitê de tecnologia da informação e, especificamente na área de segurança informação, existe uma norma que é a ISO 27005, a norma de gestão de riscos em segurança da informação. Nós já recebemos uma encomenda que é uma sugestão da Austrália de que à luz da nova ISO 31000 que vai ser lançada, a ISO 27005 que está quase igual, mas não é igual, precisa ser adaptada. Então, a tendência é que essas várias normas, da mesma forma o Brasil está prestes a lançar uma norma específica de gestão de risco no combate a incêndio na área de explosão, então você tem várias normas específicas que seriam influenciadas pela existência da ISO 31000. Assim eu

não consigo te dizer uma norma específica, mas todas as áreas - gestão em projetos de segurança, meio ambiente, área de qualidade - todas essas áreas vão de uma certa forma serem influenciadas positivamente no sentido de caminhar para essa linguagem única e algumas normas que talvez tratassem o assunto de gestão de riscos de uma certa forma pouco estruturada ou até mais informal, vão passar a contar com uma ferramenta muito poderosa para essa questão que são as duas normas tanto a de tecnologia tanto a de diretrizes.

Qual a principal diferença da ISO 31000 se comparada à Australiana e Neozelandesa 4360?

A 4360, eu diria que ela foi a semente da ISO 31000 porque o primeiro projeto foi baseado nessa norma, mas, logo em seguida, a Áustria - que tem uma norma nacional de gestão de risco - o Canadá e outros países já fizeram várias sugestões e comentários e essa norma foi tão alterada que basicamente você ainda encontra alguma coisa como, por exemplo, o processo que ficou muito parecido com o processo atual em relação a 4360, mas eu diria que a ISO 31000 é uma norma que está muito mais elaborada e desgastada envolvendo muitos especialistas. Aqui no Brasil, só no nosso comitê, são quase quinhentas pessoas atualmente e são especialistas em várias áreas que leram essa norma, criticaram essa norma, mandaram sugestões e comentários... se você imaginar que da mesma forma que acontece no Brasil acontece na Alemanha, no Estados Unidos, na Suíça, na Áustria, na Espanha, no Japão, na China e a quantidade de gente que olhou essa norma, fez sugestões. Então a norma não é burocrática, a norma não é trabalho acadêmico, a norma é algo preparado com a visão prática de "como é que a gente pode já pegar essa norma e sair usando no dia seguinte de que ela for publicada".

Como membro do Comitê Brasileiro sobre as Normas de Gestão de Segurança da Informação, da série 27000, de que forma a ISO 31000 contribuirá com esse tipo de norma ?

Ela já influência na nascência. Nesse ponto tem um comentário importante: o fato de eu, em particular, ter participado desses dois grupos tanto como delegado, coordenador da comissão gestão de riscos e também como responsável pela norma específica de gestão de risco na segurança da informação, nós tivemos a oportunidade de enviar comentários para a 27005 já deixando ela muito alinhada com a ISO 31000. Então, no fundo, o Brasil largou na frente no sentido específico da área de segurança da informação enviando diversas sugestões de comentários que fossem de alinhamento com ISO 31000 antes mesmo que norma fosse lançada. Isso se deveu, com certeza, à nossa participação nesse outro grupo.

Com relação à gestão ambiental e às normas da série 14000 como se dará a conexão com ISO 31000 ?

A gestão de risco está embutida em todas as áreas, em todos os aspectos e nessa parte do meio ambiente mais ainda. A ISO 14000 lida diretamente com todos esses impactos ambientais, impactos na sociedade, tem toda a questão de responsabilidade social... então tudo isso tem algum tipo de risco, risco de contaminar, o problema do aquecimento global... tudo isso são riscos que de uma certa forma vão passar a ser tratados de uma forma mais estruturada usando a ISO 31000.

Qual a expectativa de adoção da norma pelas corporações brasileiras ?

O nosso lançamento aqui no Brasil está planejado fazer um lançamento com uma ampla divulgação em várias cidades apresentando a norma divulgando e orientando as empresas como elas podem fazer para melhorarem a aplicação dessa norma. Então, assim que a norma for lançada aqui no Brasil vamos fazer um trabalho intensivo de divulgação que envolverá todo o comitê. Como nós temos especialistas em diferentes áreas, cada um desses especialistas vai ficar responsável por divulgar a norma dentro da sua área de especialidade, dentro do seu segmento de atuação. Nossa estratégia é distribuir este trabalho de evangelização ou de divulgação da norma ao longo de todos os membros e participantes do comitê aqui no Brasil.

Qual a vantagem das empresas que adotarem a norma?

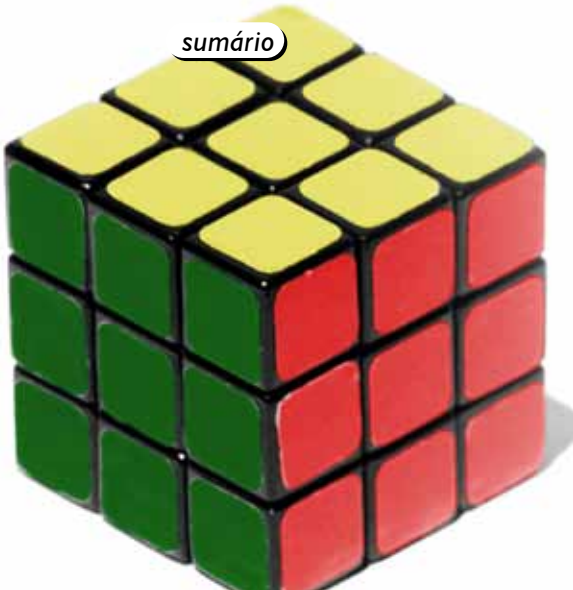
A vantagem, principalmente as que adotarem a norma logo de início, é que elas vão partir na frente. A norma é um conceito bastante inovador mas é um conceito necessário. O mercado estava precisando de uma norma para criar essa linguagem única, para criar esse padrão, esse modelo. O que essas empresas terão como vantagem é poderem ter essa ferramenta poderosa para que elas quebrem esses silos, essas ilhas de gestão de risco dentro da organização e passarem a ter uma visão mais integrada, uma visão holística para tratarem seus riscos corporativos.

Sobre a reunião que estava acontecendo, qual era exatamente o tema?

Essa reunião é a reunião regular da comissão de estudo. Normalmente a gente tem feito essa reunião no Rio de Janeiro ou aqui em São Paulo e a reunião de hoje tratou de diferentes temas que envolvem andamento de vários grupos de trabalho. Existem grupos de trabalho que falam sobre a norma de gestão de riscos de projetos, existem grupos específicos na área de gestão de continuidade de negócios, existe um dos grupos de trabalho que desenvolve normas brasileiras. Para esse grupo de trabalho existia duas tarefas importante na reunião de hoje: uma era apreciar o resultado da consulta nacional da ISO 31000, que foi aprovado, então o comitê aprovou a ISO 31000 que já tinha sido aprovada pela sociedade e fazer as revisões e acertos dos comentários finais da ISO Guia 73 que vai entrar na próxima semana em consulta nacional que fica mais trinta dias seguindo o mesmo processo, para que o lançamento de ambas as normas seja simultâneo também aqui no Brasil.

Mariana Fernandez
Editora

sumário



ACONTECE

na Brasiliano

Mariana Fernandez

FORMANDOS ANGOLANOS EM SÃO PAULO

Após a apresentação de seus trabalhos de conclusão de curso, formou-se em São Paulo, nos dias 20 e 21 de Agosto de 2009, na sede da FAPI/FESP a 1ª. Turma do Curso de Multiplicadores – Projeto de Segurança Empresarial.

Os alunos do curso de extensão universitária são colaboradores da Sonangol da área de segurança empresarial.

Ministrado inteiramente em Angola, com 440 horas/aula, o curso da Brasiliano & Associados formou onze alunos angolanos que, coordenados por Antonio Celso Ribeiro Brasiliano, estiveram em contato com as melhores ferramentas, processos e metodologia na formação qualificada de um profissional de segurança.

Resultado da integração de vários cursos na área de segurança visando qualificar a equipe de segurança com os novos processos da segurança empresarial, o curso contou com disciplinas fundamentais, como: Análise de Riscos, Investigação, Inteligência, Plano de Emergência, Auditoria, entre outras. Todos os módulos tiveram carga horária de 40 horas/aula e iniciaram em Agosto de 2008 encerrando em Maio de 2009.

Para Antonio Celso Ribeiro Brasiliano, "a equipe de multiplicadores irá multiplicar o conhecimento para todos os colaboradores ou para toda a equipe de segurança da Sonangol como um todo, em todas as suas unidades, em todas as partes do país; além de ajudar a implementar o processo de gestão de risco na segurança empresarial".

Além de Brasiliano, os alunos contaram com o conhecimento e experiência dos docentes Mário Brasil e Vitória Padovani.

Na banca examinadora, estavam presentes Antonio Brasiliano, Álvaro Takei, Vitória Padovani, Joffre Coelho e Claudio Moretti, avaliando os trabalhos de tema Projeto de Segurança Empresarial.

Para Enza Cirelli, Diretora de Treinamento da B&A, "o resultado foi positivo, atendendo às expectativas dos gestores que vieram para o Brasil para fazer a apresentação do projeto que era um case da Sonangol".

Enza explica que "cada aluno fez o trabalho final do curso de uma unidade da Sonangol, um fez da refinaria, outro da edificação sede e daí por diante; eles atenderam e seguiram o processo e atenderam às expectativas do diretor de segurança empresarial Victor Antonio Santos, que implementou o projeto acreditando no sucesso e no crescimento da equipe e ficou muito satisfeito com o resultado."

Os gestores agora estão aptos a darem continuidade à implementação do projeto.

A revista Gestão de Riscos e a Brasiliano & Associados parabenizam os formandos colaboradores da Sonangol:

Antonio de Jesus Figueiredo Torres; Antonio Mario Carvalheiro; Eduardo Tavares Maria Relvas; Fernando Ngula; Henrique António Nunes Neto; Jairo V. de Aguilar; Joaquim Botelho de Amorim; Mariana Sebastião Tomás Branco; Marisa Pilartes Caetano Domingos; Patricia Carla Diogo da Silva; Pedro Kuatikweyni

ISO 31000 NO YOU TUBE

No dia 3 de setembro de 2009, entrou no You Tube dois vídeos com palestra de Antonio Celso Ribeiro Brasiliano traçando o histórico e explicando a norma ISO 31000 - Principles and Guidelines for Risk Management, da International Organization for Standardization, a ser lançada em outubro de 2009.

O tema, até então, inédito no portal, conta agora com discurso exclusivo dividido em dois vídeos que somatizam um pouco mais de 15 minutos.

Assista aos vídeos clicando AQUI e atualize seus conhecimentos sobre a norma internacional da Gestão de Riscos.

BRASILIANO PALESTRA EM CONFERÊNCIA DE GRC

A relevância da implantação do Plano de Continuidade de Negócios em uma instituição bancária foi tema da palestra de Antonio Celso Ribeiro Brasiliano na 3ª. Edição da Conferência de Gerenciamento de Riscos Corporativos.

O evento ocorreu de 22 a 24 de setembro no Hotel Quality Moema em São Paulo e contou com participantes como as empresas Vivo, Vale, Sabesp, Merck Sharp & Dohme, Petrobrás, Clariant, Grupo Pão de Açúcar entre outras.

A Brasiliano & Associados apoiou o evento que diversificou os temas em formatos diferentes como Workshops, Painel de Debates, Palestras, discutindo casos práticos casos práticos que ilustram as dificuldades do mercado, as melhores práticas e estruturas de gestão de risco.

Os principais tópicos da conferência foram:

- *Matriz de Risco Corporativo & Mapas de Controle*
- *Técnicas de Gestão de Risco (por processo, por produto, por linha de produção)*
- *Gestão de Riscos aliada aos objetivos estratégicos da empresa*
- *Cultura de Gestão de Riscos – Uniformização de critérios e conceitos*

O evento, realizado pelo IQPC, foi uma oportunidade de novos negócios, posicionamento e relacionamento onde foram discutidas, de forma geral, as melhores práticas de gestão e estratégias para o equilíbrio entre desempenho, retorno e tolerância de riscos.

Estiveram presentes na palestra, cerca de 60 participantes, entre eles presidentes, vice-presidentes, diretores, gerentes, superintendentes, controllers e auditores atuantes nas áreas de risco de importantes corporações brasileiras.

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!!!!

b&a
BRASILIANO & ASSOCIADOS

Sede Angola: | Rua Comandante Kwenha, 2º edifício, 2º andar Cnj 21. Município das Kinachiche - Luanda - Angola
| Telefone Fixo: 244 222 008835 | Telemóvel: 244 914 656226 / 224 914 653224 / 244 929 529908 / 224 928 227713 / 224 923 609049
| e-mail: riboldi@brasiliano.com.br / mauro.ao@brasiliano.com.br / dviana@brasiliano.com.br / abrasiliano@brasiliano.com.br
| site: www.brasiliano.com.br

Gestão de Riscos Positivos: Uma Visão Inicial

André Macieira

Após anos de aplicação, a gestão de riscos vem aparecendo como um conjunto de práticas modernas e eficientes de gestão. Várias organizações já fizeram uso dessas práticas e muitas outras estão em processo de implementação. Os resultados dessas iniciativas têm sido bastante positivos.

Contudo, observa-se que recorrentemente a gestão de riscos vem sendo aplicada com foco na prevenção e tratamento de eventos de perdas. Nesse sentido, a prática revela de forma inquestionável que, no que tange a gestão de riscos, as ameaças de perdas sempre receberam maior atenção do que as oportunidades de ganhos.

Um argumento inicial que ajuda a explicar esse viés "negativo" é que o ser humano apresenta grande dificuldade ao tentar se concentrar, ao mesmo tempo, em ameaças e oportunidades. Um exemplo prático dessa dificuldade é a análise SWOT, onde são realizadas, separadamente, identificação de oportunidades e de ameaças. A essa limitação humana, em não conseguir atentar a oportunidades e ameaças a um só tempo, será dado o nome de *mind-set.*

Um outro argumento relevante, também oriundo da natureza humana, é sua tendência em atribuir maior importância, repercussão e *accountability* a uma perda ocorrida do que a um ganho não aproveitado. Em seu livro a Vantagem Competitiva das Nações, o economista

Michael Porter afirmou que "o temor da perda frequentemente é mais poderoso que a esperança da vitória".

O COSO ERM também chama a atenção para essa parcialidade. Durante a seção que trata o *Risk Assessment*, o documento cita a "*Prospect Theory*", estudo que levou um de seus dois criadores, Daniel Kahneman, a receber o prêmio Nobel de economia de 2002. Segundo essa teoria, os seres humanos estariam propensos a tomar medidas mais drásticas quando confrontados com possibilidades de perdas do que com possibilidades de ganhos.

Baseado nesses argumentos, pode-se entender por que são as ameaças de perda que levam as organizações a procurarem ferramentas de gestão para suas incertezas. Consequentemente, a gestão de riscos foca-se na mitigação de riscos de perdas em detrimento do aproveitamento dos riscos de ganhos.

Contudo, é fundamental ressaltar que não há nenhum impedimento teórico para um enfoque positivo da gestão de riscos. As principais normas para gestão de riscos, como a AS/NZS 4360, a ISO 31000 e o COSO ERM são claras a respeito da existência tanto de oportunidades quanto de ameaças.

De acordo com esse quadro, todo o investimento em complexas estruturas para gestão de riscos estaria sendo subutilizado, uma vez que diversos riscos positivos, capazes de gerar novos ganhos para a organização, simplesmente estariam passando despercebidos. Essa incapacidade de perceber tais ganhos será chamada de miopia organizacional.

Em suma, ao gerir seus riscos, as organizações se perguntam principalmente "O que pode dar errado?". Esse enfoque as impede de perceber uma grande quantidade de oportunidades potenciais a serem exploradas. No entanto, a partir do momento em elas começam a questionar "o que pode dar mais certo do que o que ocorre hoje?", essas oportunidades são identificadas, analisadas, retidas e viabilizadas de forma consciente e estruturada.

Como motivação adicional, podemos identificar diversas organizações que vêm perseguindo oportunidades de forma pouco estruturada, desperdiçando quantias significativas de capital em apostas intuitivas e otimistas e, consequentemente, apresentando um retorno financeiro aquém do esperado.

Nesse sentido, grandes investimentos vêm sendo feitos em "resultados esperados incertos", sem a utilização de ferramentas adequadas para identificação da oportunidade, avaliação dos ganhos e, principalmente, monitoração dos resultados obtidos e comunicação aos envolvidos.

Riscos Positivos: O que são?

Na gestão de riscos negativos, uma organização analisa suas fontes de risco de forma a identificar eventos (ameaças) com consequências negativas (perdas) sobre os resultados da organização.

Em oposição, na gestão de riscos positivos, as mesmas fontes de risco deverão ser analisadas. Mas dessa vez, o foco deverá ser a busca de eventos (oportunidades) com consequências positivas (ganhos) que levem a organização a alcançar resultados superiores aos obtidos atualmente.

Uma vez identificadas ameaças e oportunidades, a organização deverá, então, implementar controles. Na gestão de riscos negativos, esses controles são desenvolvidos com o objetivo de diminuir a probabilidade de concretização das ameaças e/ou diminuir as suas consequências.

A gestão de riscos positivos, em contrapartida, deverá implementar controles para tirar máximo proveito das oportunidades identificadas, elevando tanto sua probabilidade de ocorrência quanto sua consequência. A gestão de riscos negativos vê a incerteza como fonte de perda. Já, na gestão de riscos positivos ela é uma fonte de ganhos.

A distinção entre gestão de riscos negativos e positivos pode se tornar confusa caso a separação entre os conceitos de oportunidades (eventos relacionados aos riscos positivos) e ameaças (eventos relacionados aos riscos negativos) não seja clara e objetiva.

Conforme já foi dito, a diferença entre gestão de riscos positivos e gestão de riscos negativos está no foco de aplicação dado pela organização. Nesse sentido, a diferença entre uma oportunidade e uma ameaça é baseada em qual foi a intenção ou propósito da organização ao analisar as fontes de risco.

Caso a intenção seja "o que pode dar mais certo do que o que dá hoje", então o evento deve ser formulado como uma oportunidade. Caso a organização analise as fontes de risco com o propósito de encontrar "o que pode dar errado", então os eventos levantados devem ser considerados ameaças.

Essa intenção, que diferencia oportunidades e ameaças, tem um caráter subjetivo. No entanto, é bastante razoável acreditar que a maneira como um evento é entendido irá afetar o desenvolvimento dos controles propostos para seu tratamento e natureza dos ganhos resultantes. A figura abaixo ilustra esta discussão sintetizando as idéias apresentadas até então.

De forma a tangibilizar a discussão do que seria uma gestão de riscos positivos, seguem abaixo alguns exemplos de práticas de uma organização que gere riscos positivos:

- Processos de monitoração e auditoria de inovação para avaliar a efetividade da organização na identificação e aproveitamento de oportunidades;
- Implantação de controles estratégicos para maximizar a probabilidade ou a magnitude de evento com consequências positivas
- Tangibilização do grau de indução à oportunidade de uma organização (em oposição ao apetite ao risco) e à flexibilidade (em oposição à tolerância) que um analista, coordenador ou gerente pode ter para identificar e investir em oportunidades;
- Capacidade de difusão de uma cultura de incentivo à maximização do retorno esperado por uma determinada estratégia e otimização dos recursos alocados;
- Modelagem e mensuração do valor de flexibilidade e capacidade que uma organização possui para se adaptar à mudanças no ambiente interno e externo e melhorar seu desempenho alinhado à sua estratégia;
- Formalização da *accountability* de cada funcionário de uma organização para analisar as fontes de risco existentes e identificar o que pode dar mais certo do que o que vem dando hoje;
- Monitoração do "motor de geração" de resultados de uma organização, analisando quais oportunidades estão deixando de ser aproveitadas e difusão de aprendizado neste sentido para todos;

Riscos Positivos: O que não são?

Em primeiro lugar, eventos completamente inesperados que geram ganhos para a organização não podem ser confundidos com gestão de riscos positivos. Gerir riscos positivos significa tomar medidas conscientes e estruturadas para tirar proveito de incertezas. Apenas ter sorte não significa gerir riscos positivos.

Em segundo lugar, não se deve confundir a excelência em gestão de riscos negativos com a gestão de riscos positivos. Quando uma organização minimiza drasticamente seus custos maximizando sua eficiência no tratamento de possíveis ameaças, a distinção entre riscos positivos e negativos pode se tornar tênue e controversa. Dessa forma, quando uma organização olha para suas fontes de risco e avalia "qual é o menor custo possível para tratar o que pode dar errado" podem ser criados argumentos que caracterizem essa ação enquanto de criação efetiva de valor para o acionista

Também não se pode confundir a gestão de riscos positivos com a aplicação da gestão de riscos negativos nos processos estratégicos da organização. A gestão de riscos negativos, muitas vezes, envolve a coleta e reporte de uma grande quantidade de informação. Essa, muitas vezes, pode ser usada para apoiar o processo estratégico de uma organização. Isso, no entanto, consiste apenas em um uso mais nobre da gestão de riscos negativa.

Finalmente, em alguns casos, uma gestão de riscos positivos ineficiente pode parecer uma gestão de riscos negativos. Se uma organização espera que determinado evento possa acontecer e gerar ganhos, ela pode implementar controles para aumentar a probabilidade de ocorrência ou para maximizar as consequências dessa oportunidade. No entanto, se o evento não ocorre, não se pode dizer que se tratou de um risco negativo. Conforme foi discutido, a diferença entre uma ameaça e uma oportunidade está na maneira como a organização analisa as fontes de risco e formula o evento. Portanto, investir em oportunidades que não ocorrem é gerir os riscos positivos de forma ineficiente, não devendo ser confundido com gestão de riscos negativos.

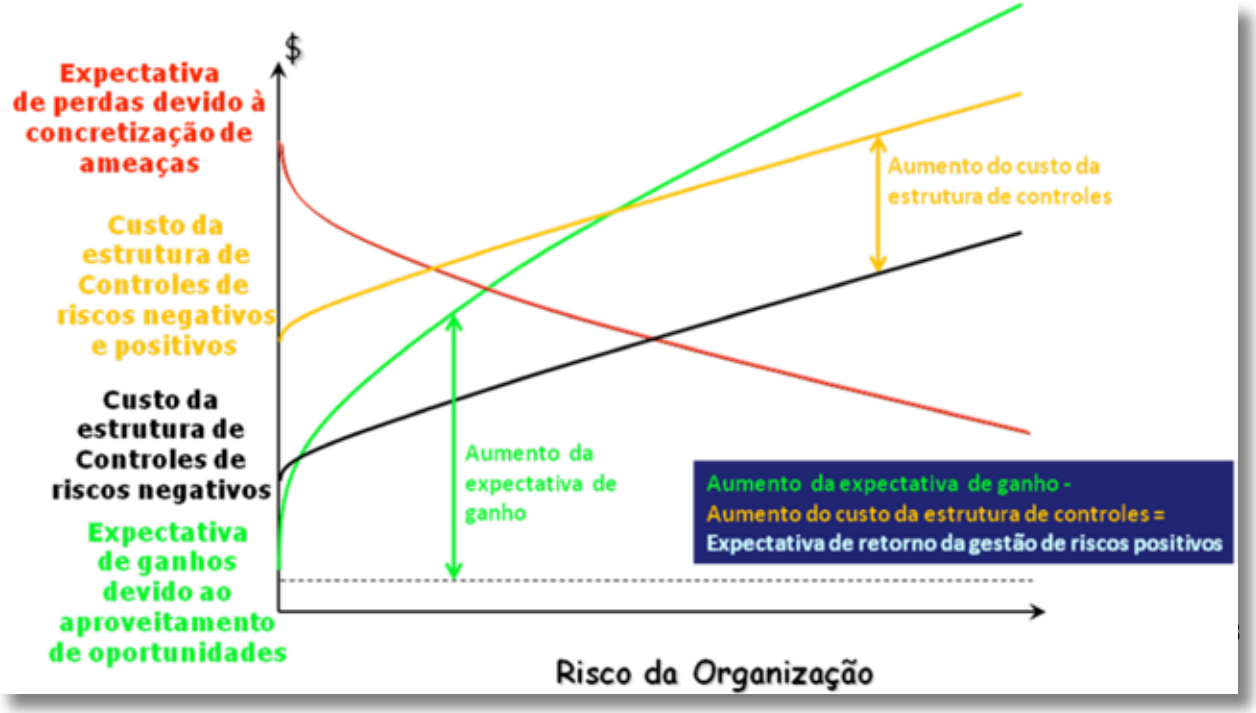
Riscos Positivos: Como gerir insights iniciais?

Um termo muito usado na literatura de gestão de riscos negativos é o apetite ao risco. Ele significa uma medida agregada de quanto risco uma organização está disposta a aceitar. Quanto menor ele for, menor será a variabilidade aceita pela organização.

Analisando a gestão de riscos positivos, poderíamos pensar em outro termo que espelhasse o conceito de apetite ao risco: a indução à oportunidade. A indução à oportunidade seria uma medida agregada de quanto uma organização estaria disposta a investir para ter maior flexibilidade no aproveitamento de oportunidades potenciais.

Como já foi dito, ter sorte não significa gerir riscos positivos. Quando uma organização vislumbra uma oportunidade e decide por aproveitá-la, ela deve implementar controles para este fim. Essa implementação quase sempre exigirá um determinado gasto. Assim, ao implementar um novo controle, a organização irá incorrer em um custo certo para obter um ganho incerto.

A figura abaixo mostra como o crescimento das expectativas de ganhos com aproveitamento de oportunidades, está relacionado com o custo da estrutura de controles que induzam a concretização dessas oportunidades. Dessa forma, uma organização necessita escolher o ponto em que deseja estar para poder decidir quais oportunidades aproveitar e quais controles implementar. Além disto, ressalta-se a idéia de que gestores e executivos estão sempre buscando meios para criar uma assimetria entre as incertezas relacionadas à indução de ganhos potenciais e à tolerância a possíveis perdas.



Como induzir uma oportunidade significa incorrer em incertezas em relação a ganhos, organizações indutoras deverão tender a ser mais flexíveis. O oposto acontece com organizações de alto apetite ao risco, que aceitam grandes riscos para não incorrer em custos fixos para controlá-los. Dessa forma, organizações com baixo apetite a risco implementariam controles que, consequentemente, as impediriam de conseguir a flexibilidade necessária para induzir suas oportunidades.

Também é importante observar que a gestão de riscos positivos estará alinhada a estratégias inovadoras. Isso porque, na medida em que uma organização identifica um possível evento de ganho e passa a criar controles com a intenção de aproveitá-lo, os ganhos obtidos em algum momento serão parte da previsão de receita planejada.

Em outras palavras, ao se perguntar "o que pode dar errado?" a organização passará a identificar a não ocorrência do ganho como uma ameaça. Assim, a variabilidade antes entendida como possibilidade de oportunidade, passará a ser descrita de maneira inversa como a possibilidade de uma ameaça.

Com isso, a atuação da organização, que antes poderia ser descrita como gestão de riscos positivos passará a ser gestão de riscos negativos. Dessa forma, uma organização só irá manter uma gestão de riscos positivos ao longo do tempo se estiver, continuamente, identificando e aproveitando novas oportunidades.

Finalmente, observa-se que a idéia de que "perfis controladores" devam ser responsabilizados pela gestão de riscos negativos e "perfis inovadores" pela gestão de riscos positivos parece ser bastante interessante. Contudo, ela pode guardar uma armadilha.

Profissionais inovadores podem ser de grande utilidade para gestão de riscos negativos na medida em que buscam formas diferentes de lidar com ameaças, conseguindo, por exemplo, implementar controles menos onerosos. Da mesma maneira, profissionais conservadores poderiam contribuir para a gestão de riscos positivos na medida em que tenderiam a evitar desperdícios em busca de oportunidades pouco viáveis.

Considerações Finais

O presente artigo está inserido no âmbito do grupo denominado ABNT/CEET Gestão de Riscos, mais especificamente em seu subgrupo 03: Estudo e discussão sobre riscos positivos (entendidos enquanto oportunidades), com o objetivo de estabelecer conceitos e métodos iniciais para uma reflexão mais aprofundada do que seria a gestão de riscos com consequências positivas, sua forma de aplicação e resultados práticos para organizações.

Aqueles interessados em participar deste grupo e receber os artigos desenvolvidos favor entrar em contato pelo e-mail andre.macieira@elogroup.com.br.

André Macieira

Mestre em Engenharia de Produção pela UFRJ; professor de gestão de riscos e estratégia empresarial em cursos de pós-graduação lato sensu (MBA) pela COPPE UFRJ; colaborador do Grupo de Produção Integrada da COPPE/UFRJ; coordenador do grupo de estudos de gestão de riscos positivos da ABNT.

sumário

A Gestão de Riscos deve permitir ao usuário contestar os dados apresentados

André Pitkowski

Um erro comum nos esforços de Gestão de Riscos Corporativos é concentrar muita atenção às solicitações da alta administração da empresa (por exemplo, metas e entregáveis), negligenciando as necessidades das pessoas que trabalham na gestão do negócio, que são a primeira linha de defesa para a Gestão eficaz do Risco.

A solução tecnológica deve ajudar a Gestão do Risco tornar-se um processo cujos dados possam ser contestáveis.

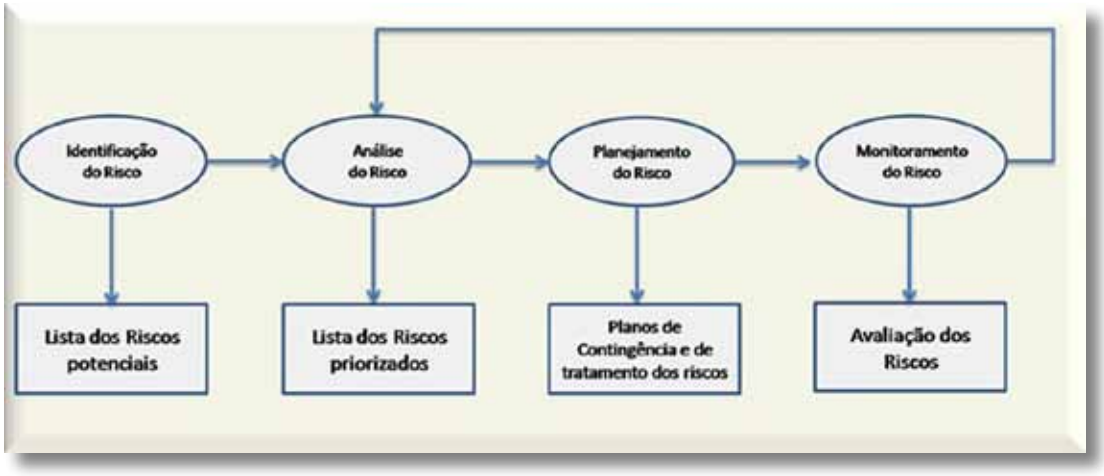
Explicando:

Criar uma solução fácil de usar por diferentes usuários, por vezes infrequentes, apresentando-lhes dados realmente relevantes em vez de forçá-los a procurar por essas informações através do sistema.

Uma maneira de oferecer dados sobre riscos que sejam relevantes para o negócio é uma Home Page na intranet (pode ser um portal também) da empresa que possa ser facilmente adaptada considerando as diferentes características dos usuários.

Por exemplo, a área de Controles Internos tem uma relação de controles que precisam de atenção juntamente com a avaliação disponível para os usuários contestarem essas avaliações e proporem Planos de Ação necessários para se manter esses controles efetivos. Todos os usuários devem ter problemas e itens de ação sobre a sua Home Page pessoal de Gestão de Riscos e saberão o quanto de esforço e atenção será exigido para a remediação.

Garantir a coerência através de todos os processos de GRC, criando usuários engajados e capacitados, em vez de frustrados e confusos com a solução pode ser melhorado com um *workflow* configurável que permita a automação de processos de revisão e aprovação das etapas da GRC, bem como a análise das causas para eventos que resultaram em perdas.



A Gestão de Riscos Corporativa deve ser capaz de:

- Apontar os riscos e falhas de compliance para as pessoas certas no momento certo;
- Monitorar as atividades de risco e compliance, acompanhando as ações subsequentes;
- Estabelecer um processo de escalação dos pontos de atenção para que os superiores responsáveis sejam notificados e estejam conscientes de quanto e quando uma ação de correção torna-se necessária;
- Um processo automatizado de notificação de gestores de negócio quando uma ação corretiva necessária falhar em sua execução de modo que medidas apropriadas possam ser executadas ainda a tempo.

A Gestão de Riscos Centralizada pode ser de grande ajuda para o usuário se a informação correta for disponibilizada num único ponto de vista, de modo a suportar a atividade a ser executada. A alternativa negativa é o usuário navegar através do sistema para encontrar as informações de causas que originaram a ocorrência do eventos, e para os usuários frequentes (ou assíduos) essa pode ser uma tarefa cansativa e frustrante.

As informações pertinentes ao GRC devem ser comunicadas para cima e para baixo permeando toda a organização, assim, o reporte é um componente crítico para se poder contestar a tempo os dados relativos ao risco. De forma a apoiar a análise, tomada de decisão e de ação, os reportes e relatórios devem ser oportunos, sucintos, precisos e flexíveis. A apresentação dessas informações é importante e deve incluir gráficos, diagramas, tendências e *dashboards*.

André Pitkowski
Consultor na área de Governança, Risco e Compliance

sumário

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.

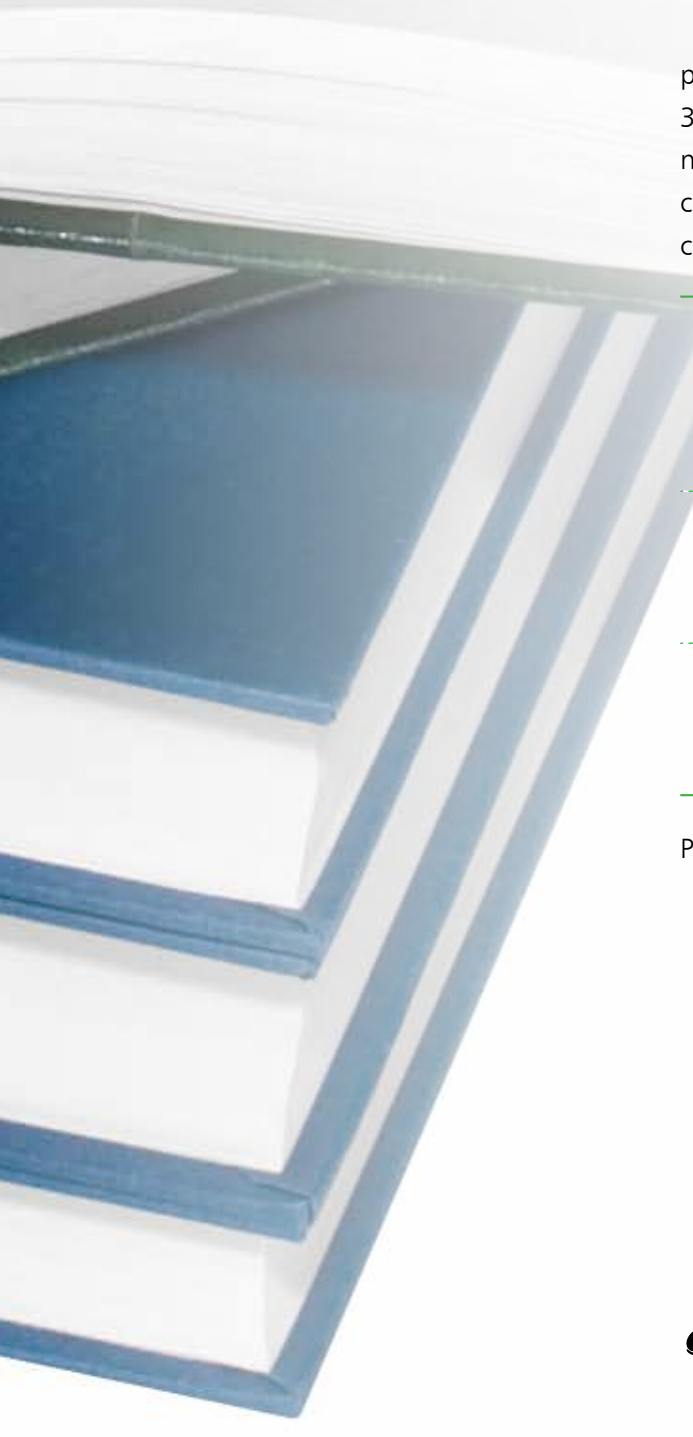
No Brasil, através da ABNT, tem as normas ABNT NBR 15999 - 1 e 2, que descrevem o processo, estrutura e conteúdo de um sistema de Gestão de Continuidade de Negócio.

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

Consulte – nos!!!!

Curso: A Nova ISO 31000 Seus principais elementos

Álvaro Takei



Conhecer a ISO 31000 passa a ser, para o Gestor de Segurança, importante atualização.

A Gestão de Riscos Corporativos, em sua sigla – GRC – já nos dá uma primeira lição dos aspectos envolvidos na visão estabelecida pela ISO 31000, uma vez que promoverá a convergência das áreas de Governança, Riscos e Complience, essa convergência, de maneira simplificada, deverá integrar importantes aspectos de cada uma das áreas, conforme quadro resumido a seguir:

G Governança	Dashboard do BSC da Gestão por Indicadores; Cobit e Itil da Governança de Tecnologia da Informação; PMBok da Gestão de Projetos.
R Riscos	ISO Guia 73 e a própria 31000 da Gestão de Riscos; ISO 27000 da Segurança da Informação; BS 25999 da Gestão de Continuidade do Negócio.
C Compliance	Normas Internas; Decretos Governamentais e dos Tribunais de Contas; Basiléia, Sox, CVM e Banco Central.

Para sintetizar podemos dizer que a ISO 31000:

- É uma orientação geral para a gestão de riscos;
- Não é específica de determinado setor ou segmento, portanto, deverá ser usada por toda e qualquer organização;
- Pode ser aplicada por toda a vida de uma organização, em uma ampla gama de atividades, incluindo estratégias e decisões, operações, processos, funções, projetos, produtos, serviços e bens;
- Aplica-se a qualquer tipo de risco, seja qual for a sua natureza, independentemente de ter consequências positivas ou negativas;

- Uma vez que fornece orientações genéricas, não se destina a promover a uniformidade da gestão de risco nas organizações. A concepção e implementação de planos de gestão de risco e frameworks levarão em conta as diferentes necessidades de uma organização específica, notadamente, os seus objetivos, contexto, estrutura, operações, processos, funções, projetos, produtos, serviços ou bens e práticas específicas empregadas;
- Pretende-se que seja utilizada para harmonizar os processos de gestão de risco nas normas existentes e futuras, oferece uma abordagem comum de apoio às normas relativas a riscos específicos e/ou setores, e não substituem as normas;
- Não se destina para fins de certificação.

Também de maneira resumida, apenas com o intuito de dar uma visão geral, podemos dizer que a ISO 31000 está fundamentada em um tripé, a saber:

I. PRINCÍPIOS DA GESTÃO DE RISCOS

A Gestão de Riscos:

I. Cria e protege valor;
II. É parte integrante de todos os processos organizacionais;
III. É parte da tomada de decisões;
IV. Aborda explicitamente a incerteza;
V. É sistemática, estruturada e oportuna;
VI. Baseia-se nas melhores informações disponíveis;
VII. É customizável;
VIII. Considera fatores humanos e culturais;
IX. É transparente e inclusiva;
X. É dinâmica, interativa e capaz de reagir a mudanças;
XI. Facilita a melhoria contínua da organização.

2 ESTRUTURA DA GESTÃO DE RISCOS (FRAMEWORK)

Esta estrutura tratará da questão do Mandato e Comprometimento interagindo com o seguinte ciclo:

1. Concepção da estrutura para gerenciar riscos;
2. Implementação da gestão de riscos;
3. Monitoramento e análise crítica da estrutura;
4. Melhoria contínua da estrutura.

3 PROCESSO DE GESTÃO DE RISCOS

Estas são linhas gerais dos principais elementos que compõe a ISO 31000. Da forma como foram apresentadas, há uma aparente simplicidade, entretanto, se analisarmos cada um dos aspectos expostos, iremos notar que há uma complexidade de assuntos, ferramentas e técnicas envolvidos, que só serão de domínio total para aqueles que estudarem.

Dessa forma, a Brasiliano e Associados, visando capacitar os profissionais do segmento, vem, há algum tempo, oferecendo cursos e palestras sobre este emergente tema. Avalie seu conhecimento, por meio deste texto, se achar que falta domínio, procure por sua atualização. Não perca tempo!

Álvaro Takei
Diretor de Ensino Digital da Brasiliano & Associados
takei@brasiliano.com.br
* Texto original do autor

sumário
treinamento

VOCÊ ESTÁ PREPARADO PARA OS NOVOS DESAFIOS DE RISCOS DO MERCADO??

PREPARE-SE !! FAÇA DIFERENÇA !!

Frequente os cursos da Brasiliano&Associados, empresa com mais de 20 anos de experiência em Gestão de Riscos Corporativos !!

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

LER & SABER

Mariana Fernandez

O MÉTODO PROFUNDO E FUNDAMENTAL DA GR

Novo livro de Antonio Celso Ribeiro Brasiliano, traz método alinhado com a ISO 31000

No mundo atual, a maioria das corporações já atentou para a necessidade imperativa de se conhecer os riscos que as afetam bem como os impactos desses mesmos riscos sobre seus negócios.

A pouca atenção que ainda se dá aos riscos que permeiam todos os níveis das atividades dos negócios resulta em "perdas financeiras, deterioração da imagem e reputação" da companhia ou o acometimento de crises.

Mas como o gerenciamento de riscos deve ser executado na administração dos riscos potenciais para que as corporações não apenas ganhem da concorrência como sobretudo sobrevivam em meio às mais variadas situações perigosas que afetam o mundo dos negócios?

O novo lançamento da Sicurezza Editora sai na frente quando o assunto é Gestão de Riscos Corporativos. A nova obra de Antonio Celso Ribeiro Brasiliano traz uma explanação aprofundada da nova norma internacional de gestão de riscos, a ISO 31000.

Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado de Análise de Riscos (Sicurezza Editora, 2009) retoma e aprofunda a famosa metodologia para aqueles que já dominam as diretrizes básicas da gestão de riscos nas empresas.

Nas palavras do autor, o livro "tem a finalidade de ajudar os gestores de riscos a implantarem um processo lógico de gestão e análise de riscos, possuindo critérios, métodos e ferramentas que já são utilizadas em inúmeras empresas no Brasil e no mundo".

Em seus treze capítulos, o Método Brasiliano Avançado fornece um processo para a identificação dos perigos, avaliação dos seus Fatores de Riscos, análise e avaliação dos riscos corporativos.

De forma detalhada, o método descreve os passos a serem percorridos, as ferramentas a serem utilizadas, os critérios a serem adotados na probabilidade e impacto, além de estabelecer a priorização das ações a serem executadas.

Além da definição e aplicabilidade da norma ISO 31000, a obra também disseca normas já conhecidas como a metodologia COSO e a ISO Guia 73. O método também utiliza ferramentas autênticas como a Matriz SWOT, a Matriz de Impactos Cruzados e o Diagrama de Ishikawa e técnicas, *check-lists* e questionários que mitigam quase que por completo o risco de não propiciar uma análise de riscos completa.

Ricamente ilustrado, a compreensão do método tende a ser absoluta aos leitores dedicados que terão a possibilidade de aplicar todo o conhecimento embasado em experiência de mais de 20 anos do autor na área de Gestão de Riscos Corporativos.

Leia sobre o framework do novo método no artigo Framework do Processo de Gestão e Análise de Riscos Corporativos – Método Brasiliano Avançado.

sumário