ISSN 1678-2496N

b&a BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

junho 2009 | edição 44

NORMAS E REGULAMENTAÇÕES

EM FOCO

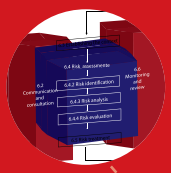
VIROU PANDEMIA. E AGORA?

OUTSOURCING

Outsourcing Ameaçado

GESTÃO DE RISCOS

Entendendo Riscos Operacionais



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** | Marina Brasiliano

Colunistas | Álvaro Takei e Mariana Fernandez. **Colaboradores desta edição** | Fernando de Bonneval de Carvalho, Gustavo Cirelli, Rosangela Aparecida Stringher, Renato Opice Blum e Camilla do Vale Jimene

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

Vivemos Na a Era da Turbulência, Mas mesmo assim temos que Vencer no Caos

O mundo está interconectado e mais interdependente do que nunca. A globalização e a tecnologia são dois fatores de risco da chamada Descontinuidade no ambiente mundial. A interdependência global atua em favor de todos nos bons tempos, mas também difunde, rapidamente, as dores e os danos nos maus tempos.

No livro "Vencer no Caos", os autores Philip Kotler e John Caslione afirmam que a nova normalidade é a convivência com níveis de riscos e incertezas altos, tendo em vista a a velocidade da magnitude dos choques. Portanto o ponto focal é a sobrevivência!!

Kotler e Caslione ainda ressaltam que as empresas devem conviver com os riscos, que são mensuráveis e com a incerteza, que é imensurável. Para tanto, precisam construir sistemas de monitoração sensíveis, sistemas de construção de cenários e, principalmente sistemas de respostas rápidas, para gerenciar nestes períodos turbulentos. A constatação dos autores é que as empresas, INFELIZMENTE, operam sem sistema de gestão do caos. Isso mesmo: Sistema de Gestão do Caos!! As empresas devem criar sistemas que reduzam os riscos e respondam à incerteza.

A turbulência produz dois importantes efeitos. De um lado, cria vulnerabilidades, contra as quais as empresas precisam de uma blindagem defensiva. Do outro, gera oportunidades a serem exploradas. O mar revolto pode ser mau para uns e bom para outros, depende da reação e do preparo!

Um sistema de gestão do caos deve ajudar a empresa a manobrar, executar e prosperar na nova era em que estamos ingressando: A Era da Turbulência!

A pergunta é: em qual dos dois efeitos você estará enquadrado? Vulnerabilidade ou oportunidade?

Vai depender do seu preparo em gestão de riscos e construção de cenários prospectivos, matérias ainda incipientes em inúmeras empresas!!

Boa leitura e sorte.

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

b&a
BRASILIANO & ASSOCIADOS

TODO RISCO É INERENTE AO NEGÓCIO

a DIFERENÇA é saber GERENCIÁ-LO

Para a sua empresa poder **SURFAR** nas ondas do **MERCADO**, há necessidade de você compreender a dinâmica dos riscos. 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.

informações | www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

EDITORIAL

Por que ser Correto?

Na Justiça o empregado sempre tem razão? Nem sempre. Quem contrata serviços terceirizados se isenta de responsabilidade no pagamento dos direitos dos subcontratados? Nem sempre, pelo menos até agora, que o projeto de lei que prevê a responsabilidade solidária no pagamento dos direitos trabalhistas ainda não foi aprovado.

Por que um projeto de lei que pode acabar com o outsourcing está em processo de votação na Câmara do Deputados? Porque os empresários brasileiros, em geral, não se preocupam em verificar a idoneidade das empresas que firmam parcerias; não tomam para si a responsabilidade de respeitar o trabalhador terceirizado como respeitam os seus próprios. Muito dessa atitude impensada dá-se pela inexperiência na subcontratação de empresas que faz o barato sair caríssimo após o processo de reclame de horas extras, insalubridade e etc.

Nesta edição da revista Gestão de Riscos a insegurança jurídica na terceirização é tema de uma matéria imprescindível a todos os médios e grandes empresários e gestores.

Além dos riscos jurídicos, a RGR deste mês aborda riscos operacionais, análises comparativas de normas e processos de gestão de risco além dos riscos digitais, caracterizando vítimas e criminosos.

Atualíssima, a revista digital da Brasiliano & Associados aborda a anunciada pandemia de Gripe A, agora oficial. Há PCN que salve? É o que falaremos a seguir. Assim como da importância da realização dos testes no planejamento da continuidade de negócios.

Na coluna Treinamento, o fim da polêmica: MBA ou Pós-Graduação? Por que é um excelente diferencial para os gestores de risco?

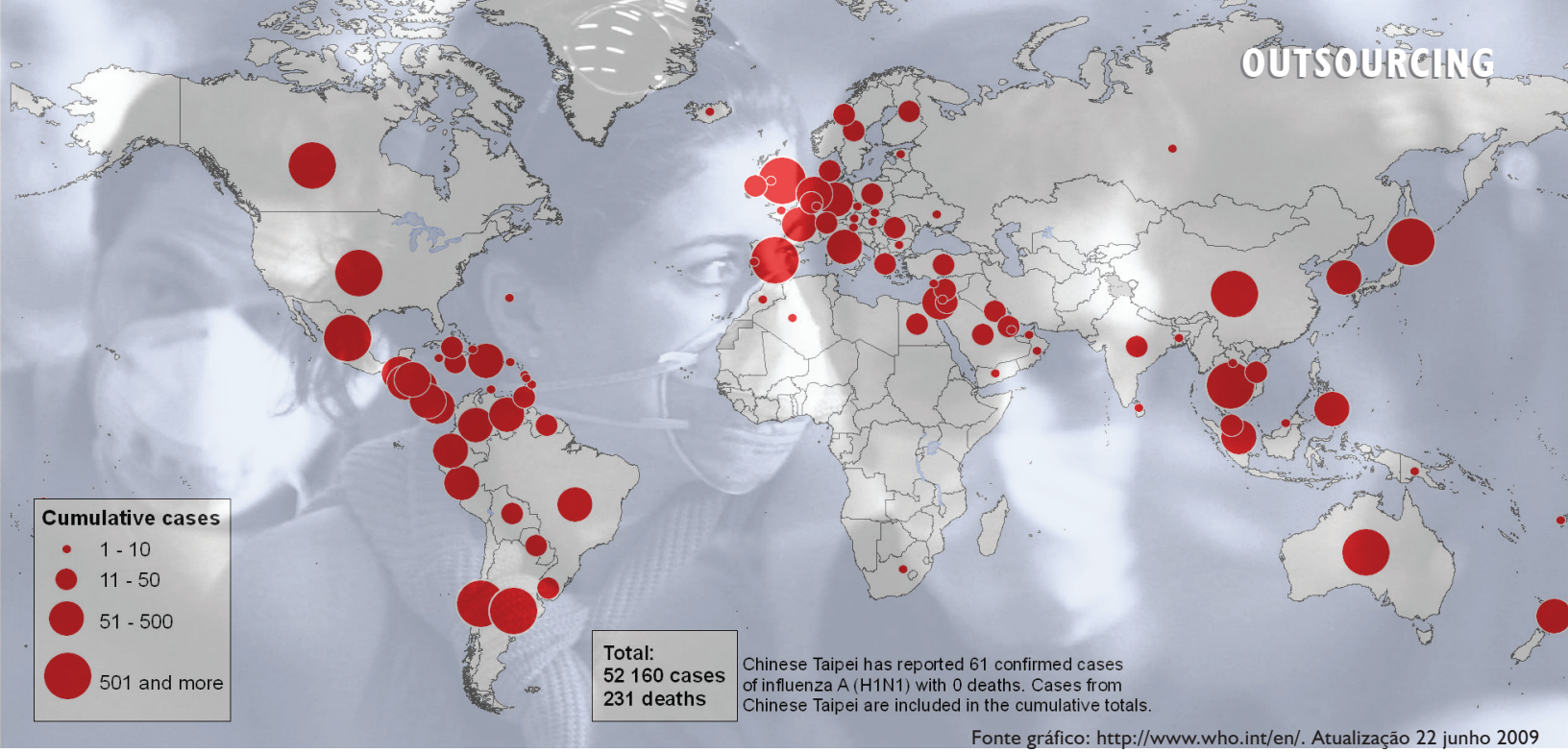
Para os gestores de risco é feita nossa revista; a cada dia com um empenho maior para levarmos a todos os nossos leitores o conteúdo mais responsável e atual sobre o gerenciamento de riscos corporativos.

Obrigada pela confiança e boa leitura!

Boa leitura!

Mariana Fernandez
Editora da Gestão de Riscos

b&a
BRASILIANO&ASSOCIADOS



Fonte gráfico: http://www.who.int/en/. Atualização 22 junho 2009

Virou Pandemia. E agora?

Mariana Fernandez

O que muda com a oficialização do período de pandemia da gripe A? Há PCN que resolva?

Na última edição, em entrevista, o especialista em Business Continuity Plan Antonio Celso Ribeiro Brasiliano falava do medo da OMS em "declarar pandemia no mundo". Um dia antes da oficialização, em entrevista à agência France Press, o francês Antoine Flahault, diretor da Faculdade de Altos Estudos de Saúde Pública, dizia que a OMS deveria declarar oficialmente o nível 6 "o mais rápido possível" já que "a nível epidemiológico" a pandemia já havia começado, não havendo mais como negar os fatos.

Um dia depois da declaração - mas não por interferência dela -, em 11 de junho de 2009, a OMS aumentou o nível para 6, caracterizando a pandemia. No momento do decreto eram registrados 27.737 casos de gripe A no mundo e 141 mortes.

A decisão foi motivada pelo aumento dos casos de infecção pelo vírus nos EUA, Europa, Austrália, América do Sul e em outros lugares. Mais cedo, o governo da Suécia já havia informado a imprensa da decisão da OMS.

Trata-se, agora oficialmente, da primeira epidemia global de gripe em 41 anos.

A fase seis, que se traduz em que uma epidemia global está em andamento, significa que já há focos que se contagiam em nível comunitário em pelo menos outro país de uma região diferente

da primeira na qual foi detectado, no caso, o vírus A(H1N1).

O especialista em epidemias de gripe, Keiji Fukuda, porta-voz da OMS, declarou na ocasião que "isso não significa que o vírus tenha se tornado mais grave, que a doença seja mais séria e que a taxa de mortalidade tenha aumentado". Ou seja, não muda nada em relação ao combate à doença; o fato significa apenas que o vírus se espalhou por muitos países e que medidas globais devem ser tomadas para combatê-lo.

A OMS pediu na ocasião, que as nações não fechem suas fronteiras nem restrinjam viagens e comércio.

De acordo com o especialista Antoine Flahault, a OMS não havia declarado pandemia até a data de sua declaração porque estava preocupada em não criar pânico, levando em consideração a virulência relativamente fraca do vírus, equivalente ao da gripe comum. Flahault compreende que "o plano não deve gerar consequências excessivas e inapropriadas" já que "o vírus não é o H5N1 da gripe aviária, não tem a mesma virulência (H5N1: 60% de letalidade), nem representa a mesma problemática".

Antonio Celso Ribeiro Brasiliano, tem opinião um pouco diversa; acredita que a demora deveu-se a "questões políticas", já que os primeiros focos disseminadores e os que mais crescem em infectados são os países de primeiro mundo. "O impacto da pandemia mais a recessão poderia ser catastrófica", completa o especialista. Para Brasiliano, o fato de o "nível de agressividade do vírus" ser baixo, também influenciou no adiamento da OMS, que "não quis que o impacto econômico fosse grande em função de paralizações e transtornos com o fechamento de fronteiras, como estaria previsto nas ações emergenciais".

A PANDEMIA AGRAVA O PROBLEMA NO BRASIL?

De acordo com a ministra interina da Saúde, Márcia Bassit, em entrevista ao site G1, a fiscalização nos portos, aeroportos

Pandemia, do grego pan = tudo/ todo(s) e demos = povo, é uma epidemia de doença infecciosa que se espalha entre a população localizada em uma grande região geográfica como, por exemplo, um continente, ou mesmo o planeta.

De acordo com a Organização Mundial da Saúde, uma pandemia pode começar quando se reúnem estas três condições:

**** O aparecimento de uma nova doença à população.***

**** O agente infecta humanos, causando uma doença séria.***

**** O agente espalha-se fácil e sustentavelmente entre humanos.***

Uma doença ou condição, não pode ser considerada uma pandemia somente por estar difundido ou matar um grande número de pessoas; deve também ser infeccioso. Por exemplo, câncer é responsável por um número grande de mortes, mas não é considerada uma pandemia porque a doença não é contagiosa (embora certas causas de alguns tipos de câncer possam ser).

A Organização Mundial de Saúde (OMS) desenvolveu um plano de preparação de gripe global que define as fases de uma pandemia, esboços no papel da OMS, e faz recomendações para medidas nacionais antes e durante uma pandemia.

e fronteiras vai continuar do jeito que está assim como o diagnóstico rápido da doença. Isso porque o Brasil avalia que essa rede de monitoramento da nova gripe está funcionando muito bem.

"Essa nova fase de alerta não significa maior gravidade dos casos. A letalidade dessa doença no mundo é de 0,5% e é considerada muito baixa pela OMS. A transmissão no Brasil permanece limitada e sem sustentabilidade. O Brasil se antecipou a todas as medidas recomendadas pela OMS. Por isso, essa nova situação que foi anunciada hoje, não muda em nada, absolutamente nada os procedimentos que o governo brasileiro adotou para vigilância para o diagnóstico e o tratamento da doença. A população pode ficar absolutamente tranquila mesmo com um anúncio deste fato hoje de que estamos numa pandemia", declarou a ministra.

Para Antonio Celso Ribeiro Brasiliano, contudo, "as empresas devem ter em mente a questão das rápidas mudanças em situações de pandemia", e, por isso, "não devem entrar em pânico mas também não devem relaxar". No que tange ao risco das corporações, levanta duas questões estratégicas que podem complicar a vida das empresas. Para ele, mesmo se tratando de uma doença "branda", as empresas correm o risco de "ter partes de seus efetivos de rh com gripe, podendo ter paralizações parciais". Outro fator, ocorre "se houver mutação do vírus e ele ficar forte e resistente", segundo ele "isto poderá causar interrupções graves nos negócios". Para isso, o especialista aconselha as empresas e seus respectivos fornecedores e parceiros a considerarem o risco da "evolução da pandemia", preparando-se para o enfrentamento do cenário.

MUDANÇAS NO PCN?

O PCN é o planejamento da continuidade das operações integradas com ações de crise e de emergência. Segundo Brasiliano, "a situação pandêmica declarada pela OMS não diferencia na prática da situação pré-pandêmica." O especialista adverte que "o importante é as empresas terem os PCN operacionais, testados e em condições de darem o start a qualquer momento".

Brasiliano ensina que as empresas devem "ficar em alerta monitorando de forma contínua a evolução da situação" e capacitarem-se a trabalhar com menor força de trabalho, adequando seus planos de continuidade de negócio a no mínimo "três

PERÍODO DE INTERPANDEMIA

**** Fase 1: Nenhum novo subtipo de vírus de gripe foi descoberto em humanos.***

**** Fase 2: Nenhum novo subtipo de vírus de gripe foi descoberto em humanos, mas uma doença, variante animal ameaça os humanos.***

PERÍODOS DE ALERTA DE PANDEMIA

**** Fase 3: Infecção (humana) com um subtipo novo mas nenhuma expansão de humano para humano.***

**** Fase 4: Pequeno(s) foco(s) com transmissão de humano para humano com localização limitada.***

**** Fase 5: Maior(es) foco(s) mas expansão de humano para humano ainda localizado.***

PERÍODO DE PANDEMIA

**** Fase 6: Pandemia: aumenta a transmissão contínua entre a população geral.***

cenários: efetivo pequeno com pandemia, efetivo médio (20% a 30%) e efetivo grande (60% a 75%)."

"O ponto de gargalo são os processos considerados críticos. As empresas devem saber com clareza como estes processos vão rodar em situações de descontinuidade", acrescenta.

A NOVIDADE: VACINA BRASILEIRA

No Brasil, o vírus da nova gripe encontrado em pacientes infectados no estado de São Paulo é ligeiramente diferente do encontrado na Califórnia, Estados Unidos, o primeiro a ser isolado depois do aparecimento da doença, conforme anunciou no último dia 16 de junho o Instituto Adolfo Lutz, da Secretaria de Estado da Saúde de São Paulo

Por essa razão, a vacina, que já está sendo desenvolvida para a nova gripe a partir do sequenciamento nos Estados Unidos, pode servir para o vírus encontrado no Brasil. "A proteína da matriz é igual. Identificamos pequenas mudanças na hemaglutinina. É possível vislumbrar que as alterações não sejam grandes e que a vacina possivelmente será protetora para ele", explicou Clélia Aranda, coordenadora de Controle de Doença da secretaria.

Até o último dia 15 de junho, o país contava com 74 casos confirmados, sendo 27 deles em São Paulo; haviam também 79 casos suspeitos e 480 descartados.

Mariana Fernandez
Editora da Revista Gestão de Riscos da Brasiliano&Associados

sumário

Outsourcing AMEAÇADO

Mariana Fernandez

Projeto de lei prevê responsabilidade solidária para as empresas praticantes da subcontratação no pagamento de processos trabalhistas

A prática do outsourcing pode tornar-se inviável no País caso seja aprovado o projeto de lei que está prestes a ser votado na Câmara dos Deputados. O texto do projeto prevê a "responsabilidade solidária", ou seja, ambas as empresas, contratante e contratada serão consideradas de equivalente responsabilidade com o trabalhador, o qual terá o direito de escolher a quem quer processar.

Os trabalhadores terceirizados são os únicos que não contam com proteção prevista em lei. Por isso, a referência dos juízes do Trabalho tem sido a Súmula 331 do Tribunal Superior do Trabalho (TST) de 1995.

Súmula é um verbete que registra a interpretação pacífica ou majoritária adotada por um Tribunal a respeito de um tema específico, com a dupla finalidade de tornar pública a jurisprudência para a sociedade bem como de promover a uniformidade entre as decisões. A Súmula em questão prevê a chamada "responsabilidade subsidiária", o que quer dizer que caso a terceirizadora não responda pelos encargos trabalhistas requisitados pelo trabalhador, fica a cargo da empresa contratante arcar com as despesas.

Primeiramente, o texto do projeto previa a "responsabilidade subsidiária", tornando lei a decisão da maioria dos juízes, porém, por causa de um destaque votado em separado foi imposta a "responsabilidade solidária", conforme informou o deputado Sandro Mabel (PR-GO) ao jornal O Estado de São Paulo.

Mas "os dois [tipos de responsabilidade] estão em vigência. Quem decide se é uma ou se é outra é o juíz quando prorroga a sentença. Cada caso é um caso. Tem caso que é subsidiária e tem caso que o juíz vai entender que é solidária", explica o analista judiciário José Marcio Zaidan Faneco, que há 22 anos trabalha na Justiça do Trabalho.

Do ponto de vista do processo, "a única diferença (da subsidiária) pra solidária, é que é um pouquinho mais rápido para se cobrar. Na

subsidiária você tem que esgotar primeiro a empresa terceirizada pra depois passar pra contratante", explica Faneco.

A iniciativa que visa regular o trabalho terceirizado deve-se à essa demora na fase de cobrança dos processos em que o juíz opta pela responsabilidade subsidiária e, que, por isso, podem arrastar-se por anos em prejuízo do trabalhador.

Porém, "se for tudo solidário acaba a terceirização. Porque vai todo mundo querer entrar com processo contra a empresa rica. Vai ser inviável", sentencia Faneco.

MITIGANDO OS RISCOS DE PROCESSO

Da forma com que vêm sendo utilizados o outsourcing e a terceirização no Brasil, não há preocupação da empresa contratante em saber se a empresa terceirizada é idônea. "Não há uma responsabilidade social de jeito nenhum", declara o analista. "Se não fosse por isso, essa subsidiariedade, é aí que ninguém receberia nada mesmo; por isso que o juíz ataca por esse lado, por isso que a Justiça do Trabalho faz isso", completa.

A empresa tomadora de serviço geralmente recorre para não pagar a conta, porque, em tese, pagou à subcontratada o suficiente para que os direitos dos trabalhadores fossem honrados. Contudo, recorrer, no caso de a responsabilidade passar para a empresa tomadora de serviço, é algo que não dá muito resultado, pois, segundo Faneco, os argumentos da empresa são muito frágeis, já que esta não possui os documentos necessários para a comprovação de sua inocência, como: cartão de ponto, holerites, etc.

A solução, então, para os gestores, é estudar muito bem a empresa a que se vai destinar certa área da corporação, verificando se tem capacidade para, além de desempenhar o serviço a que se propõe com qualidade, garantir que os direitos de seus funcionários sejam respeitados.

Outra dica é verificar se a empresa contratada possui patrimônio para ser penhorado caso entre em falência, pois, se nada for encontrado tanto em rendimentos líquidos quanto em patrimônio, a empresa contratante será condenada a pagar os direitos trabalhistas desrespeitados pela contratada. Segundo Faneco, há casos em que as empresas terceirizadas são quase "empresas fantasma": alugam um imóvel qualquer para ser a sede, têm somente veículos arrendados e seus sócios não têm nada em nome deles. Por isso a importância da investigação antes da subcontratação.

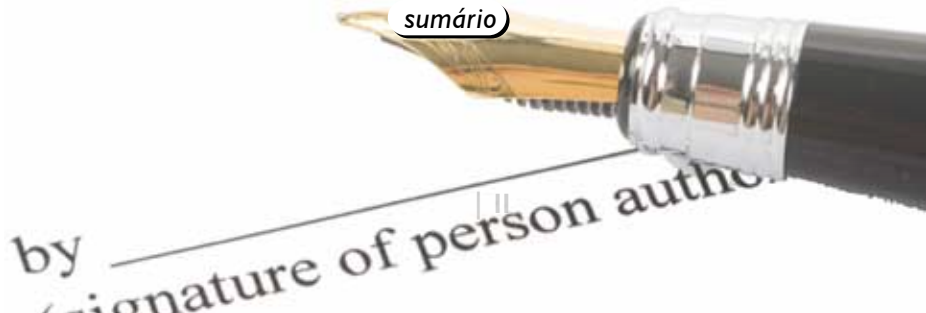
SISTEMA MISTO

A Confederação Nacional da Indústria (CNI) e a Força Sindical propõem um novo texto que, segundo eles, agradará a todos, prevendo um sistema misto. Neste, caso a empresa contratante fiscalize a contratada, sua responsabilidade é subsidiária, se não o fizer, no entanto, é solidária. Tal sistema consta de um anteprojeto de lei em análise no Ministério do Trabalho.

Faneco não acredita que a adoção do sistema misto mudaria muita coisa. Segundo ele, é uma faca de dois gumes, podendo beneficiar quem não fiscalizou e prejudicar quem o fez. Neste sistema, a empresa contratante terá dificuldades em provar que fiscalizou a contratada mas também terá uma chance maior de ser absolvida, mesmo não tendo fiscalizado.

Mariana Fernandez
Editora

sumário



COSO X ISO 31000

Fernando de Bonneval de Carvalho

O objetivo deste artigo é verificar as semelhanças e diferenças entre as normas COSO e ISO 31000 (que sairá em outubro de 2009). Assim sendo, serão apresentadas as definições de cada norma para depois constatar suas diferenças e semelhanças.

O objetivo do COSO (*Comittee of Sponsoring Organizations of the Treadway Commission*), norma criada em 1992, é o controle interno, ou seja, elaborar um processo para garantir, com razoável certeza, que sejam atingidos os objetivos das empresas.

Para gerar uma norma universal que englobasse os diferentes conceitos de gestão de riscos, foi criada a norma ISO 31000 *"General Guidelines for principles and implementation of risk management"*. A partir de sua criação foi possível generalizar a gestão de risco independentemente do tipo, tamanho e área de atuação da organização. Seu o objetivo é lidar com a incerteza que pode afetar os objetivos empresariais

Quando falamos em COSO estamos falando de Controle Interno, que compreende o plano da organização e o conjunto coordenado de métodos e medidas, adotados pela empresa, para: proteger seu patrimônio, verificar a exatidão e a fidedignidade de seus dados contábeis, promover a eficiência operacional e encorajar a adesão à política traçada pela administração.

Um dos objetivos (de quem?) é buscar através da norma, a eficiência e eficácia operacional. Aqui esta categoria (qual?) está relacionada com os objetivos básicos da entidade, inclusive

com os objetivos e metas de desempenho e rentabilidade, bem como a segurança e qualidade dos ativos.

Outro ponto da norma é a confiança nos registros contábeis e financeiros, pois, toda transações devem ser registradas e todos os registros devem refletir transações reais, consignadas pelos valores e enquadramento corretos. A empresa, também, deve buscar a conformidade com as leis e normativos aplicáveis à entidade e sua área de atuação.

Pelo COSO, o Controle Interno é um processo constituído de componentes, que estão inter-relacionados e presentes em si:

- **Ambiente Interno:** é a consciência de controle da entidade, sua cultura de controle. O ambiente de controle é efetivo quando as pessoas sabem quais são suas responsabilidades, os limites de sua autoridade e se têm a consciência, a competência e o comprometimento de fazerem o que é correto da maneira correta. A postura da alta administração desempenha papel determinante, pois deve deixar claro para seus colaboradores quais são as políticas, os procedimentos, o código de ética e o código de conduta a serem adotados. As funções principais do controle interno estão relacionadas ao cumprimento dos objetivos da entidade. Portanto, a existência de objetivos e metas é essencial para a existência dos controles internos;
- **Fixação de objetivos:** A avaliação de riscos permite que uma organização considere até que ponto eventos em potencial podem impactar a realização dos objetivos. A administração avalia os eventos com base em duas perspectivas: probabilidade e impacto. Geralmente, a avaliação utiliza uma combinação de métodos qualitativos e quantitativos, onde os impactos positivos e negativos dos eventos em potencial devem ser analisados isoladamente ou por categoria em toda a organização. Os riscos devem ser avaliados em suas características inerentes e residuais;
- **Avaliação de gerenciamento de riscos:** é um processo contínuo e que flui através da organização. Tal processo é conduzido pelos profissionais em todos os níveis da organização e deve ser aplicado à definição das estratégias da entidade. Assim, a entidade forma uma visão de portfólio de todos os riscos a que está exposta. O gerenciamento dos riscos é formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a organização, e para administrar os riscos de acordo com o apetite ao risco da entidade. Assim sendo, esse gerenciamento é capaz de propiciar uma garantia razoável para o conselho de administração e a diretoria executiva de uma organização. O gerenciamento do risco é então orientado para a realização dos objetivos em uma ou mais categorias distintas, mas dependentes.
- **Resposta ao risco:** Aqui a administração deve determinar como ela responderá aos riscos: evitando, reduzindo, compartilhando ou aceitando. Ao considerar a

A ISO 31000 foi criada com o objetivo de ser uma norma genérica de gerenciamento de riscos, aplicável em qualquer tipo de organização independente do tamanho e ramo de atividade. Sua metodologia visa identificar e analisar os riscos e os cenários que serão enfrentados.

própria resposta, a administração avalia o efeito sobre a probabilidade de ocorrência e o impacto do risco, assim como os custos e benefícios. Com isso, é possível selecionar a resposta que mantém os riscos residuais dentro das tolerâncias a risco desejadas. A administração pode, também, identificar as oportunidades que possam existir, e assim, pode obter uma visão de riscos em toda a organização;

- **Atividade de Controle:** são as políticas e os procedimentos que contribuem para assegurar que as repostas aos riscos sejam executadas. Essas atividades ocorrem em toda a organização, em todos os níveis e em todas as funções, pois compreendem uma série de atividades diversas como: aprovação, autorização, verificação, reconciliação, revisão do desempenho operacional, revisão da segurança dos bens e segregação das responsabilidades
- **Informação e comunicação:** as informações são identificadas, coletadas e comunicadas de forma coerente e no prazo, a fim de permitir que as pessoas cumpram com suas responsabilidades. Os sistemas de informática empregam dados gerados internamente e informações de fontes externas, possibilitando dessa forma, esclarecimentos para o gerenciamento de riscos e tomadas de decisão baseadas em dados relacionados aos objetivos. A comunicação eficaz ocorre ao fluir em todos os níveis da organização, onde todo o pessoal recebe uma mensagem clara da alta administração (Endomarketing), alertando que as responsabilidades do gerenciamento de riscos corporativos devem ser levadas a sério. Dessa forma, cada colaborador entende sua função no gerenciamento de riscos corporativos, assim como as atividades individuais que se relacionam com o trabalho dos demais. Os colaboradores devem, então, adotar uma maneira de passar as informações dos escalões inferiores aos superiores.
- **Monitoramento:** serve para monitorar o gerenciamento dos riscos avaliando-se a presença e o funcionamento de seus componentes ao longo do tempo. Essa tarefa é realizada mediante atividades contínuas de monitoramento, avaliações independentes ou uma combinação de ambas. O monitoramento ocorre no decurso normal das atividades de administração.

Já a norma ISO 31000 foi criada com o objetivo de ser uma norma genérica de gerenciamento de riscos, aplicável em qualquer tipo de organização independente do tamanho e ramo de atividade. Sua metodologia visa identificar e analisar os riscos e os cenários que serão enfrentados. A norma pode ser aplicada a vários tipos de riscos, por exemplo: financeiro, operacional, de saúde, de projeto, de meio ambiente, de informação, de segurança empresarial, entre outros. A norma serve para fazer com que as empresas não tratem os riscos de forma isolada, de modo que possa haver um estudo de impactos cruzados entre as diversas áreas da organização.

Assim sendo, a norma 31000 visa estabelecer uma linguagem comum e padronizar as melhores práticas, para assim, criar a convergência, ou seja, a norma visa a criação de uma gestão integrada dos riscos das diferentes áreas de uma organização. Cada risco levantado deve se atrelar ao fator de risco - onde a ferramenta acaba sendo escolhida pela empresa. O processo de gestão de riscos segundo a norma 31000 é dividido em sete etapas:

- **Comunicação e consulta:** é importante desenvolver um plano de comunicação com as partes internas e externas envolvidas, logo no primeiro estágio do processo. A comunicação envolve diálogo entre as partes, tendo como foco a consulta e não somente a comunicação de via única. A comunicação, interna e externa, eficaz é importante para que os responsáveis pela implementação da gestão de riscos e os investidores compreendam quais são as decisões tomadas e por que determinadas ações são necessárias;
- **Contexto:** é o ambiente no qual a organização está inserida, compreendendo os tipos: estratégico; organizacional; de gestão de riscos; de critérios (qual metodologia será utilizada); de estrutura e de variáveis incontroláveis;
- **Identificação dos riscos e perigos:** para se ter uma visão efetiva dos riscos e de seus fatores, existe a necessidade de se realizar uma avaliação das condições de segurança da empresa. Após conhecer o contexto em que a organização está inserida, é possível definir quais os riscos que devem ser estudados. A identificação deve incluir todos os perigos, estejam ou não sob o controle da Unidade de Negócio. O objetivo é gerar uma lista abrangente de eventos que possam afetar a organização. Após identificar os riscos, a organização deve identificar quais são seus fatores de risco;
- **Análise de riscos:** verifica o grau de criticidade dos riscos através de sua probabilidade de ocorrência e impacto na organização. Aqui usamos critérios prospectivos, pois os critérios projetivos não levam em conta o contexto atual em que a organização está inserida;
- **Avaliação de riscos:** calculamos o grau de probabilidade através da fórmula GP= fator de riscos (FR) x exposição (E). Após obtermos o Grau de Probabilidade e seu impacto é possível criar uma matriz de vulnerabilidade para cada risco;
- **Tratamento dos riscos:** dependendo do risco, a organização poderá, através de sua avaliação e análise, reter, reduzir, transferir, explorar ou até mesmo evitar o

risco. Assim, a organização cria planos de ação com o objetivo de propor soluções possíveis para mitigar os riscos e reduzir suas consequências;

- **Monitoramento:** serve para acompanhar se as medidas do Plano de Ação estão surtindo o efeito desejado e para verificar o nível de riscos identificados através de seus fatores de riscos.

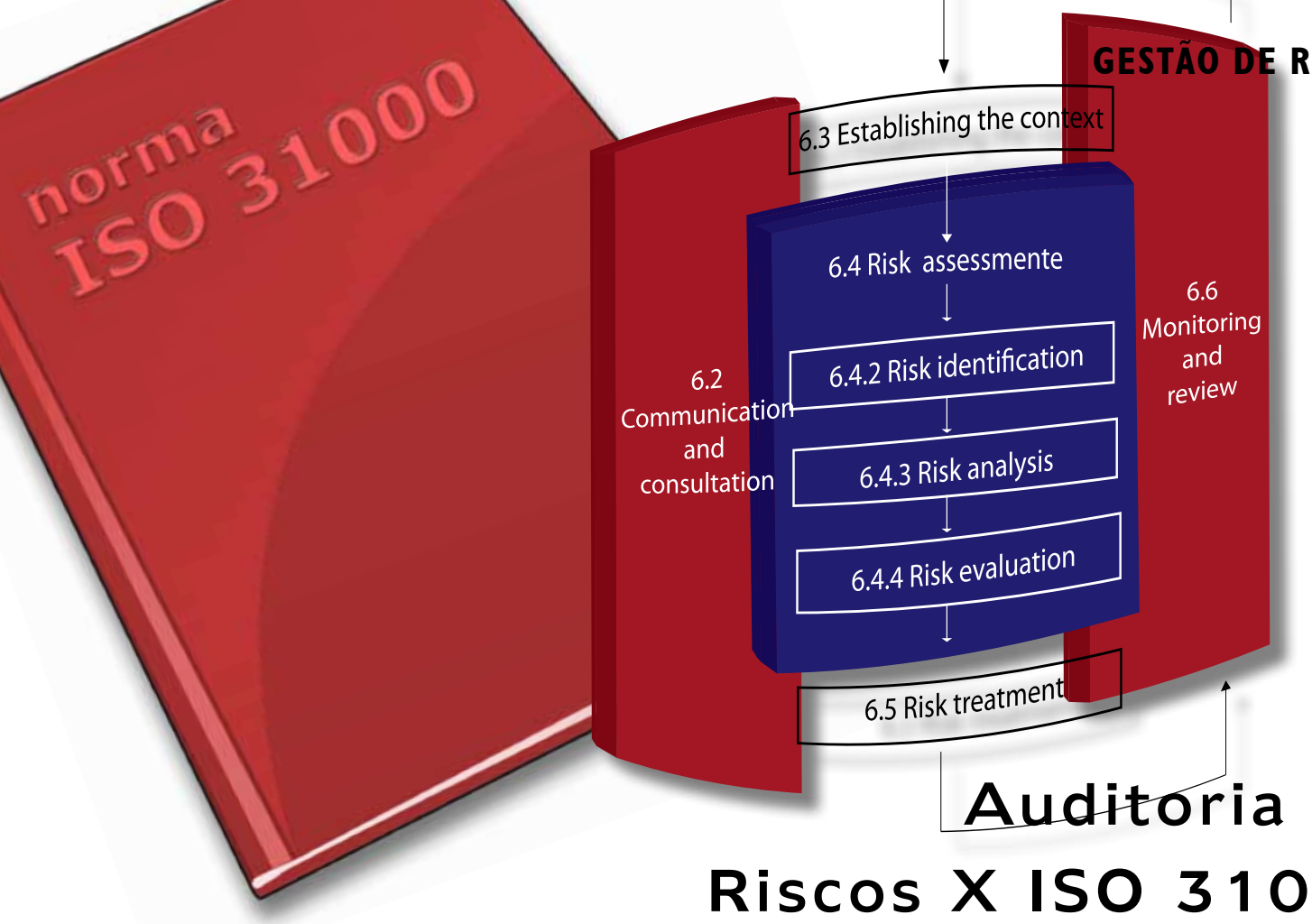
Levando em conta o framework de cada norma:

ISO 31000	COSO
1. Comunicação	1. Ambiente Interno
2. Contexto	2. Fixação de Objetivos
3. Identificação do Risco	3. Identificação de Eventos
4. Análise de Riscos	4. Avaliação de Riscos
5. Avaliação dos Riscos	5. Resposta ao Risco
6. Tratamento do Risco	6. Atividade de Controle
7. Monitoramento (indicadores)	7. Comunicação
	8. Monitoramento

Apesar de existirem semelhanças entre as normas ISO 31000 e COSO - como a identificação de riscos x identificação de eventos, análise de riscos x avaliação de riscos, monitoramento e comunicação -, o foco de cada uma é diferente. A norma 31000 tem um processo com foco principal no risco que afeta a empresa, com o objetivo de mitigá-los, assumi-los ou evitá-los. Já a norma COSO tem um processo com foco principal no controle, para garantir a eficiência e eficácia do monitoramento das atividades que irão tratar os riscos.

Fernando de Bonneval de Carvalho
Consultor da Brasiliano & Associados
fbonneval@brasiliano.com.br

sumário



Auditoria De Riscos X ISO 31000

Gustavo Vedove

Norma, por definição internacional, é um documento estabelecido por consenso e aprovado por um organismo reconhecido; que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando a obtenção de um grau ótimo de ordenação em um dado contexto. (Fonte: ABNT).

A Gestão de Riscos é o processo de mitigação – diminuição da probabilidade de ocorrência - dos perigos, que colocam em exposição os processos da instituição, evitando perdas. Visa diminuir perdas, sob todos os aspectos, tornando a empresa mais competitiva. (Antonio Celso Ribeiro Brasiliano).

Neste artigo, descreveremos as fases aplicadas na auditoria baseada em riscos corporativos frente à futura norma de gestão de riscos, batizada de ISO 31000.

ISO 31000

A nova norma ISO 31000 tem como base a norma Australiana AS/Nzs 4360:2004 de Gestão de Riscos. Com lançamento previsto para outubro deste ano, ela provém do consenso entre

trinta e cinco países após um longo trabalho iniciado em 2005.

Seu desafio é estabelecer uma linguagem comum, além de padronizar melhores práticas e abordagens para implementação. Visando essa finalidade, traz como proposta a ação de convergir informações de normas existentes (Figura 1), ou seja, padronizar termos e definições pertinentes à gestão de riscos corporativos.

Poderá ser aplicada em qualquer organização, independentemente do tipo, tamanho ou área de atuação.

A ISO 31000 busca integrar todo o processo de gestão de riscos da empresa, mudando os conceitos tradicionais que prevêem a atuação independente de cada área. Em seu framework, a norma recomenda que todas as áreas da empresa interajam com um mesmo objetivo. Para isso, traz uma linguagem comum, ou seja, a definição de uma metodologia igual para todas as áreas.

Além de abordar uma visão diferenciada, a norma terá aplicabilidade em diversos tipos de riscos. Ela também insere em seu contexto as oportunidades para o negócio. Outro ponto relevante na ISO 31000 é a recomendação em considerar sempre os fatores humanos.

Para melhor compreensão de seu escopo, segue abaixo as fases do respectivo framework:

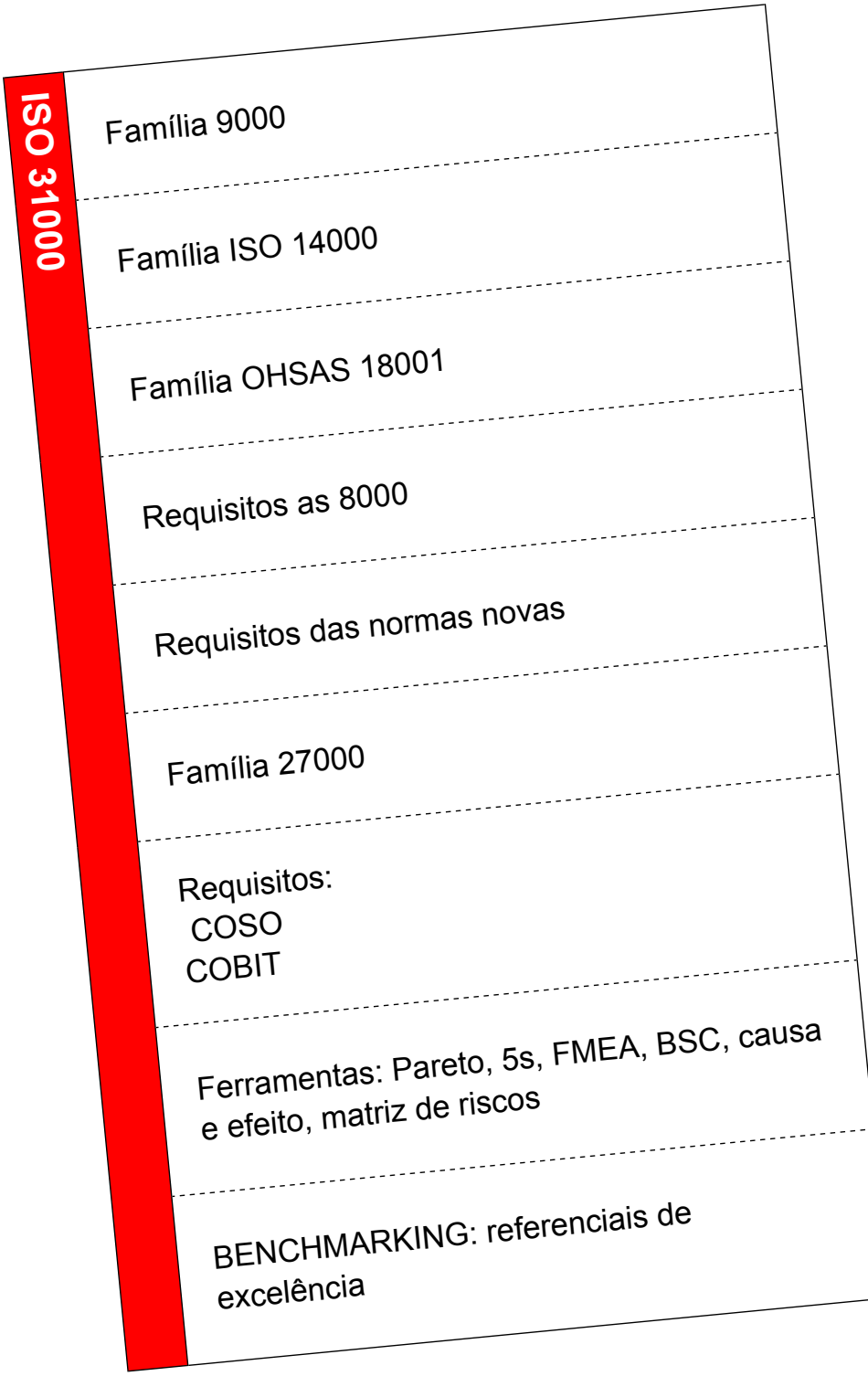


Figura 1

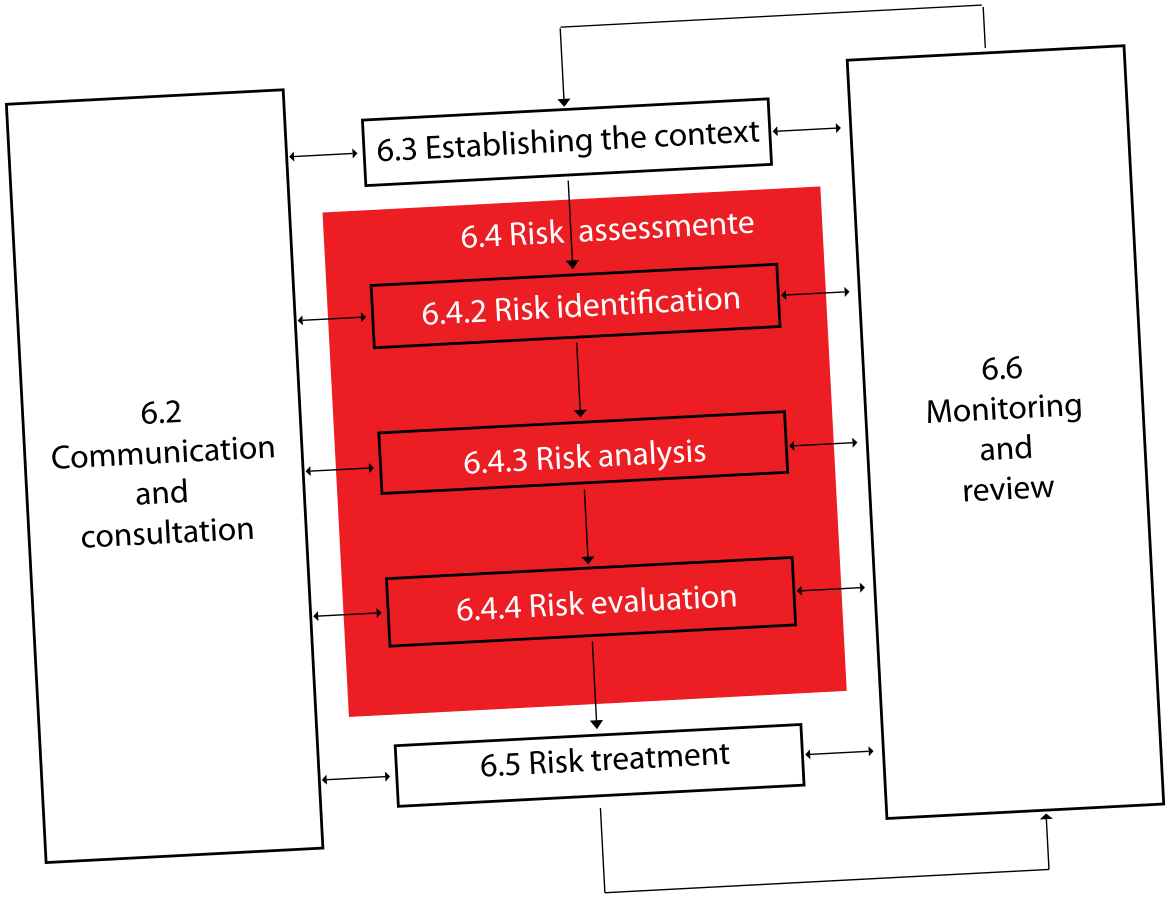


Figura 2 - Risk management process

Todo o processo é contínuo, com o objetivo de estabelecer melhorias.

É provável que, futuramente, a ISO 31000 seja um parâmetro claro a ser seguido pelas organizações, até mesmo pela grande expectativa de tornar-se uma norma certificadora.

Caso isso ocorra, as empresas que desejarem obter a certificação deverão atender cada detalhe de todas as fases da norma, abaixo demonstradas de forma resumida:

- *Comunicação e consulta:* a comunicação e consulta é uma fase constante durante todo o processo de gestão de riscos. Por isso é importante o desenvolvimento de um plano de comunicação.
- *Contexto:* é a compreensão do ambiente no qual a organização está inserida,.
- *Identificação dos riscos e perigos:* a norma exige a identificação dos riscos e seus fatores de risco, contudo não fala claramente como isso será feito.
- *Análise de riscos:* a norma exige a identificação da probabilidade de ocorrência e impacto, porém não fala claramente como isso será feito.
- *Avaliação de riscos*: Matriz de Risco.
- *Tratamento dos riscos:* exige a criação de planos de ação para os riscos.
- *Monitoramento:* recomenda que os riscos sejam monitorados, mas não fala claramente como isso será feito.

A norma fala claramente o que será exigido, porém não apresenta metodologias a serem seguidas pela empresa.

AUDITORIA BASEADA EM RISCOS

Bem diferente da auditoria tradicional, a auditoria baseada em riscos tem seu foco totalmente voltado para os riscos da empresa. Essa nova visão traz diferenças importantes no tratamento da auditoria dentro do processo da gestão de riscos da empresa; com focos diferenciados como: foco no negócio, baseado no processo, no cliente e na gestão de riscos - é um processo totalmente auditado por gestores da empresa em vez de auditores externos, como na visão tradicional. A nova visão busca auditar somente controles relevantes aos riscos identificados através do processo de gestão de riscos da empresa, buscando uma gestão antecipatória. O quadro ao lado demonstra diferenças entre a visão tradicional e a visão futura na tratativa de auditoria baseada em riscos.

Foco nos controles	Foco nos riscos
Testes com base em programa de trabalho; endereçando objetivos de controle padrão	Testes com base nos risco de negócio, identificados no levantamento de informações
Testes de todos os controles	Testes focalizados; somente dos controles que minimizam os riscos relevantes
Inspecionar, detectar, e reagir aos riscos de negócios	Antecipar e prevenir riscos de negócios na origem
Maior parte do tempo gasto em testes, validação e consolidação	Maior parte do tempo gasto em levantamento e análise de informação

AUDITORIA BASEADA EM RISCOS X ISO 31000

Todo o processo da auditoria baseada em riscos está ligado à obrigatoriedade da empresa em obter um processo de gestão de riscos. Por se tratar de uma auditoria que tem seu foco voltado somente para o risco, todo o processo da ISO 31000 se faz necessário, ou seja, o auditor se baseia no processo de gestão de riscos aplicado na empresa para a realização de seu trabalho.

"A auditoria baseada em riscos corporativos contribui para o esforço da administração no sentido de manter os processos de negócio leves e eficientes ao longo do tempo, evitando desta forma o efeito "cebola" (efeito que possui inúmeras camadas), da gestão tradicional centrada só em controles."(Antonio Brasiliano)

Gustavo Vedode
Consultor da Brasiliano & Associados
gvedove@brasiliano.com.br

sumário

ACONTECIMENTOS

Mariana Fernandez

A norma da convergência

A norma de gestão de riscos, ISO 31000, foi tema da palestra de Antonio Celso Ribeiro Brasiliano na noite do último dia 16 de junho no Hotel Campobelo Plaza.

Com uma platéia de 70 participantes de diversas corporações, o especialista em gestão de riscos discursou sobre a norma a ser lançada em outubro deste ano, que tem como base a australiana AS/NZS 4360:2004.

A norma tema da palestra oferecerá um novo padrão internacional de Gestão de Riscos, independentemente da área ou segmento de atuação das empresas.

Durante o evento, Brasiliano ressaltou o diferencial da norma ao fornecer o processo, "estabelecendo os passos para que as organizações possam, de forma equilibrada, operacionalizar seus processos de Gestão de Riscos".

O palestrante detalhou o framework da ISO 31000, que adiciona etapas às do COSO e ressaltou a "submissão e internalização" como "mecanismos que a instituição deverá utilizar para aculturar seu público, interno e externo".

Antonio Celso Ribeiro Brasiliano é o criador do Método Avançado de análise e Resposta aos Riscos Corporativos – Método Brasiliano, alinhado com a futura norma ISO 31000.

b&a
BRASILIANO&ASSOCIADOS

TOP SECRET

1º TURMA DO BRASIL

MBA em Gestão de Riscos:

FRAUDES EMPRESARIAIS

Disciplinas:

- ☑ Modelagem de Processos;
- ☑ Regulação e Normatização;
- ☑ Controles Internos e Auditoria Baseada em Riscos;
- ☑ Questões legais da Fraude;
- ☑ Perícia Eletrônica;
- ☑ Fraudes Informatizadas;
- ☑ Metodologia e pesquisa científica;
- ☑ Inteligência fiscal;
- ☑ Taxionomia da fraude e plano de prevenção;
- ☑ Investigações Empresariais.

Docentes:

Antonio Celso Ribeiro Brasiliano, Camila Vale, Carlos Eduardo, Claudio Salatini, Fábio Ribeiro, Giuliano Giova, Joffre Coelho Chagas Junior, Maxwell Martins e Vitória Padovani.

Local das Aulas:

FAPI FACULDADE DE ADMINISTRAÇÃO SÃO PAULO

Entendendo Riscos Operacionais

Antonio Celso Ribeiro Brasiliano

I. CONCEITO DE RISCO

Vamos iniciar este artigo definindo, diante de inúmeras visões, o conceito de risco. O termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender por "risco" a possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às "perdas" quanto aos "ganhos", com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações:

"Quando investidores compram ações, cirurgiões realizam operações, engenheiros projetam pontes, empresários abrem seus negócios e políticos concorrem a cargos eletivos, o risco é um parceiro inevitável. Contudo, suas ações revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e oportunidade". (Bernstein, P., p. VII, 3a edição,1996)

O risco pode ser definido como a combinação da probabilidade de um acontecimento com suas consequências (ISO/IEC Guide 73). O simples fato de existir atividade abre a

possibilidade de ocorrência de eventos ou situações que, consequentemente, trazem ou oportunidades para obter vantagens (lado positivo), ou ameaças ao sucesso (lado negativo).

Um evento é um incidente ou uma ocorrência, gerada com base em fontes internas ou externas, que afeta a realização dos objetivos. Os eventos podem causar impacto negativo, positivo ou ambos. Os que geram impacto negativo representam riscos. Pela definição COSO, "o risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos".

Os eventos que causam impacto desfavorável são obstáculos à criação de valor ou desgastam o valor existente. Os exemplos incluem paradas no maquinário da fábrica, incêndio e perdas de créditos. Eventos de impacto negativo podem originar-se em condições aparentemente positivas, como nos casos em que a demanda de produto pelo consumidor é superior à capacidade de produção, o que provoca o não atendimento da demanda, o desgaste na fidelidade do cliente e o declínio de pedidos futuros.

Eventos de impacto positivo podem tanto contrabalançar os impactos negativos como representar oportunidades. Segundo a definição COSO, oportunidade é definida da seguinte forma:

"Oportunidade é a possibilidade de que um evento ocorra e influencie favoravelmente a realização dos objetivos".

As oportunidades favorecem a criação ou preservação de valor. A direção da organização canaliza as oportunidades para seus processos de fixação de estratégias ou objetivos, formulando planos que visam o seu aproveitamento.

2. OBJETIVOS ESTRATÉGICOS E PERFIL DE RISCO

Os objetivos estratégicos orientam o modo como a organização deverá trabalhar para agregar valor a todos que investiram na organização - o que depende crucialmente do perfil dos riscos corporativos.

A definição do perfil de riscos é prerrogativa do conselho de administração que, por sua vez, reflete a posição dos acionistas. O perfil de riscos significa o nível de exposição ao risco que se aceita incorrer, envolvendo tanto apetite quanto tolerância a riscos.

O perfil de riscos deverá estar refletido na cultura da organização e, para isto, cabe ao conselho de administração outorgar um mandato claro para que a diretoria o administre. A implantação de um modelo

de Gestão de Riscos Corporativos requer o envolvimento ativo de ambos (conselho de administração e diretoria), aprimorando o processo de tomada de decisão da organização, tanto no contexto da elaboração do seu planejamento estratégico, como na sua execução e monitoramento.

Para determinar o perfil de riscos de uma organização são necessárias definições claras dos tipos de riscos, suas categorias, indicadores de desempenho e índices de volatilidade, os quais deverão ser divididos em dois grupos: um de natureza financeira (valor de mercado, geração de caixa operacional, distribuição de dividendos, etc.) e outro de natureza qualitativa (transparência, idoneidade, reconhecimento de marca, ambiente de trabalho, responsabilidade socioambiental, etc.)

3. CLASSIFICAÇÃO DE RISCOS

Não há um tipo de classificação de riscos que seja consensual, exaustivo e aplicável a todas as organizações; a classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades de sua indústria, mercado e setor de atuação. Por exemplo: os estoques de materiais de consumo são menos relevantes para um banco do que para uma indústria, onde podem representar um dos principais fatores de risco. Analogamente, as variáveis relacionadas ao "risco de mercado" são cruciais para um banco e podem não ser tão relevantes para determinada organização manufatureira.

O IBGC sugere a seguinte classificação de riscos, conforme a matriz abaixo:

		Tipos	Natureza dos Riscos		
			Estratégico	Operacional	Financeiro
origem dos eventos	Externo	Macroeconômico			
		Ambiental			
		Social			
		Tecnológico			
		Legal			
	Interno	Financeiro			
		Ambiental			
		Social			
		Tecnológico			
		Conformidade			

A Norma de Gestão de Riscos da FERMA – *Federation of European Management Associations* - sugere a seguinte classificação:

Estratégico - Relacionado com os objetivos estratégicos da organização a longo prazo. Podem afetar por áreas, como risco de: disponibilidade de capital, soberania e políticos, alterações jurídicas e regulamentares, reputação e alteração do meio ambiente físico.

Operacional - Relacionado com os assuntos quotidianos com os quais a organização é confrontada quando se esforça para atingir os seus objetivos estratégicos.

Financeiro - Relacionado com a gestão e controle eficazes dos meios financeiros da organização e com os efeitos de fatores externos como, por exemplo, disponibilidade de crédito, taxas de câmbio, movimento das taxas de juro e outros tipos de orientações do mercado.

Gestão do conhecimento - Relacionados com a gestão e controle eficazes dos recursos do conhecimento e com a produção, proteção e comunicação destes. Essa categoria engloba fatores externos, como: utilização não autorizada ou abusiva da propriedade intelectual, falhas de energia na zona e tecnologia competitiva. Do lado dos fatores internos podem referem-se a avarias nos sistemas ou à perda de funcionários-chave.

Conformidade - Relacionados a temas como saúde e segurança, meio ambiente, práticas comerciais, proteção do consumidor, proteção de dados, assuntos regulamentares e legislação laboral.

Na área bancária, os riscos são classificados como: estratégicos, financeiros e operacionais.

Ponto importante, é que, seja qual for a classificação utilizada, em todas elas, o risco operacional sempre aparece. Portanto, esse tipo de risco deve ser muito bem entendido além de possuir critérios e indicadores claros para sua avaliação.

4. RISCO OPERACIONAL

No setor financeiro, o termo risco operacional foi provavelmente usado pela primeira vez em 1995, como tentativa de explicar a inesperada e quase inacreditável falência do Banco Barings.

A definição de risco operacional ainda é causa de debates, provavelmente em função da amplitude de sua conceituação. Podemos ter as seguintes definições:

Risco Operacional - Basiléia: perdas diretas ou indiretas, resultantes de eventos externos ou de inadequações ou falhas em processos internos, pessoas e sistemas.

Risco Operacional – IBGC: os riscos operacionais estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e atos terroristas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais.

Risco Operacional – Culp – 2001: Os problemas relacionados a riscos operacionais surgem em função da inadequada atenção destinada a processos ou sistemas, ou ainda porque as pessoas falham no desempenho de suas atividades ou suas atribuições são mal especificadas.

Risco Operacional – Crouhy – 1998: É o risco de eventos externos, ou deficiências de controles internos e sistemas de informação, resultarem em perdas, estando associado ao erro humanos, falhas em sistemas e procedimentos e controles inadequados.

Risco Operacional – Hoffman – 1996: Riscos operacionais se relacionam a todas as fases do processo de negócios, desde sua originação até a execução e entrega, abrangendo a linha de frente, o apoio intermediário e o back-office.

As diferentes visões mostradas são muito esclarecedoras tanto quanto à amplitude dos riscos operacionais como quanto à sua relevância.

Acontecimentos como o tsunami em dezembro de 2004, o ataque terrorista de 11 de setembro de 2001, a invasão do centro de pesquisa da Aracruz Celulose pelo MST, em março de 2006, o ataque do PCC, em maio de 2006 em São Paulo, o apagão aéreo em no Brasil em março de 2007, as enchentes em São Paulo em março de 2009 e as enchentes no norte do Brasil em maio de 2009, são exemplos de riscos operacionais que interromperam o fornecimento de serviços, destruíram conhecimento organizacional e informações relevantes ou causaram prejuízos materiais.

Os riscos operacionais transcendem todas as linhas de negócios, sendo mais amplos do que os riscos usualmente cobertos por seguros e do que as falhas de controle. Estão presentes seja no negócio regulado ou não; seja centralizado ou descentralizado; seja conduzido através de rígidos procedimentos ou pouco controle; seja demandante de alta tecnologia ou empregue tecnologias convencionais; se realiza as vendas através de um simples canal ou através de vários canais.

Abaixo uma tipificação específica de riscos operacionais, com o objetivo de haver uma clara identificação. Portanto as principais sub-áreas do risco operacional são:

1 - Risco de Overload

Este pode ser definido como o risco de perdas por sobrecargas nos sistemas elétrico, telefônico, de processamento de dados, etc. Exemplos: 1) Sistemas não operacionais em agências bancárias, por acúmulo de informação nos canais de comunicação com a central de atendimento; 2) Linhas telefônicas constantemente ocupadas.

2 - Risco de Obsolescência

Este pode ser definido como o risco de perdas pela não substituição freqüente dos equipamentos e *softwares* antigos. Exemplos: 1) Versões atualizadas de *softwares* não compatíveis com *hardware* antigo; 2) Impossibilidade de integrar sistemas computacionais desenvolvidos em versões de *softwares* diferentes.

3 - Risco de Presteza e Confiabilidade

Este pode ser definido como o risco de perdas, pelo fato de informações não poderem ser recebidas, processadas, armazenadas

e transmitidas em tempo hábil e de forma confiável. Exemplos: 1) Situações onde informações consolidadas sobre exposição de um banco não podem ser obtidas em tempo hábil para análise; 2) Impossibilidade de prestar informações precisas em determinados horários devido à atualização de bancos de dados ocorrer por processamento em *batch*.

4 - Risco de Equipamento

Este pode ser definido como o risco de perdas por falhas nos equipamentos elétricos, de processamento e transmissão de dados, telefônicos, de segurança, etc. Exemplos: 1) Redes de micros contaminados por vírus; 2) Discos rígidos danificados; 3) Telefonia não operacional por falta de reparos.

5- Risco de Erro Não Intencional

Este pode ser definido como o risco de perdas em decorrência de equívoco, omissão, distração ou negligência de funcionários. Exemplos: 1) Mal atendimento de correntistas (má vontade, falta de informação, etc.); 2) Posicionamento da tesouraria no mercado contrário ao especificado pelo Comitê de Investimentos.

6 - Risco de Fraudes

Este pode ser definido como o risco de perdas em decorrência de comportamentos fraudulentos (adulteração de controles, descumprimento intencional de normas da empresa, desvio de valores, divulgação de informações erradas, etc.). Exemplos: 1) Desvio de dinheiro de agência bancária; 2) Aceitação de "incentivos" de clientes para conceder crédito em valores mais elevados.

7 - Risco de Qualificação

Este pode ser definido como o risco de perdas pelo fato de funcionários desempenharem tarefas sem qualificação profissional apropriada à função. Exemplos: 1) Uso de estratégias de hedge com derivativos, sem conhecimento por parte do operador das limitações desta; 2) Cálculo de perdas & lucros em carteiras, sem conhecimento dos mercados; 3) Iniciar operações em mercados "sofisticados", sem contar com equipes *(back-office* e *front-office*) devidamente preparadas.

8 - Risco de Produtos & Serviços

Este pode ser definido como o risco de perdas em decorrência da venda de produtos ou prestação de serviços ocorrer de forma indevida, ou sem atender às necessidades e demandas de clientes. Exemplos são dados por: 1) Envio de cartões de crédito sem consulta prévia ao cliente; 2) Recomendar a clientes de perfil conservador o investimento em fundos de derivativos alavancados diante de um bom desempenho no passado recente destes mesmos fundos.

9 - Risco de Regulamentação

Este pode ser definido como o risco de perdas em decorrência de alterações, impropriedades ou inexistência de normas para controles internos ou externos. Exemplos: 1) Alteração de margens de garantia ou de limites de oscilação em bolsas de derivativos sem aviso antecipado ao mercado; 2) *Front-office* responsável pela operação do *back-office*.

I0 - Risco de Modelagem

Este pode ser definido como o risco de perdas pelo desenvolvimento, utilização ou interpretação incorreta dos resultados fornecidos por modelos, incluindo a utilização de dados incorretos. Exemplos: 1) Utilizar software comprado de terceiros, sem conhecimento de suas limitações; 2) Utilizar modelos matemáticos, sem conhecimento de suas hipóteses simplificadoras.

I1- Risco de Liquidação Financeira

Este pode ser definido como o risco de perdas em decorrência de falhas nos procedimentos e controles de finalização das transações. Exemplos: 1) Envio e/ou recebimento de divisas em praças com diferentes fusos horários, feriados,regras operacionais, etc.

I2 - Risco Sistêmico

Este pode ser definido como o risco de perdas devido a alterações no ambiente operacional. Exemplos: 1) Alteração abrupta de limites operacionais em bolsas, levando todas as instituições financeiras a dificuldades; 2) Modificação repentina de base de cálculo de tributos corporativos.

I3 - Risco de Concentração (operacional)

Este pode ser definido como o risco de perdas por depender de poucos produtos, clientes e/ou mercados. Exemplos: 1) Bancos que só operem financiando clientes de determinado segmento (por exemplo, setor automotivo, crédito a lojistas, etc.).

I4 - Risco de Catástrofe

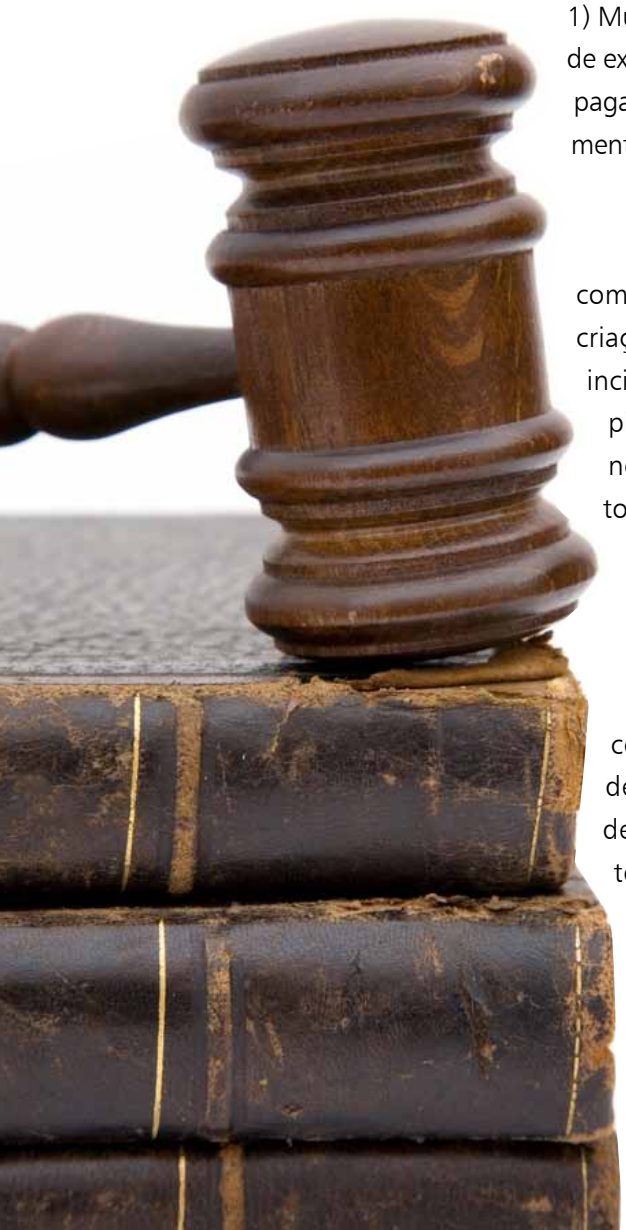
Este pode ser definido como o risco de perdas devido a catástrofes (naturais ou não). Exemplos: 1) Desastres naturais (enchentes) que dificultem a operação diária da instituição ou de áreas críticas como centros de processamento, de telecomunicações, etc. 2) Destruição do patrimônio da instituição por desastres que abalem a estrutura civil de prédios (colisão de aviões, caminhões, etc.), incêndios, etc.

I5 - Risco Legal

O risco legal pode ser definido como uma medida numérica da incerteza dos retornos de uma instituição, caso seus contratos não possam ser legalmente amparados por falta de representatividade por parte de um negociador, por documentação insuficiente, insolvência ou ilegalidade. As principais subáreas do risco legal são:

15.1 Risco de Legislação

Este pode ser definido como o risco de perdas decorrentes de sanções por reguladores e indenizações por danos a terceiros por violação da legislação vigente. Exemplos: 1) Multas por não cumprimento de exigibilidades; 2) Indenizações pagas a clientes por não cumprimento da legislação.



15.2 Risco Tributário

Este pode ser definido como o risco de perdas devido à criação ou nova interpretação da incidência de tributos. Exemplos: 1) Criação de impostos novos sobre ativos e/ou produtos; 2) Recolhimento de novas contribuições sobre receitas, não mais sobre lucros.

15.3 Risco de Contrato

Este pode ser definido como o risco de perdas decorrentes de julgamentos desfavoráveis por contratos omissos, mal redigidos ou sem o devido amparo legal. Exemplos: 1) Pessoa sem poder para assinar contratos representando a instituição; 2) Não execução pronta de garantias, requerendo o acionamento do jurídico; 3) Responsabilidades cobertas nos contratos de terceirização colocadas de forma pouco objetivas.

A classificação acima não fecha portas, muito pelo contrário, o objetivo é ajudar na identificação e categorização dos riscos. Fica claro que a classificação depende das características do negócio, por esta razão é importante uma definição objetiva. Por exemplo o risco legal em muitas empresas são categorizados a parte, sendo um tipo de risco específico.

5. CONCLUSÃO

O risco operacional deve ser avaliado de forma consistente, cabe a diretoria das empresas, seu presidente e respectivo conselho de administração estarem sensibilizados e conscientes que estes representam uma significativa ameaça aos objetivos da organização.

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

sumário

A Nova Polêmica: Vítimas ou Criminosos nos Meios Digitais?

Renato Opice Blum e Camilla do Vale Jimene

A nova discussão que acirra os ânimos dos juristas consiste na surpreendente tese que prevê a reação em legítima defesa das vítimas aos ataques criminosos de crackers, justificada sob os institutos do Direito Penal.

A polêmica é grande e as correntes de pensamento são conflitantes, considerando-se a quantidade de lesados que ingressam no judiciário buscando a punição dos criminosos virtuais e a diligente busca para afastar a sensação de vulnerabilidade nos meios eletrônicos.

Para facilitar, usaremos um exemplo demonstrando a aplicação das teses mais discutidas: imaginemos que uma grande corporação teve seus sistemas invadidos, tendo seus dados sigilosos "furtados" por um cracker; ao constatar-se vítima, a corporação aciona o departamento de Tecnologia da Informação, que localiza o criminoso através dos rastros deixados e invade seus sistemas, trazendo de volta os dados "furtados".

Sob uma primeira análise leiga a conduta acima seria justa, contudo sob o aspecto legal, a questão não é tão simples assim:

A primeira tese defendida por alguns juristas é a legítima defesa, respaldada no Código Penal, ou seja, não há crime quando o ato é praticado em legítima defesa. Ora, vale lembrar que não estamos diante de um marginal armado na iminência de atirar e, em reação, esfaqueamos o agressor para preservarmos nossa vida. No exemplo, estamos em âmbito digital e temos à disposição todo o ordenamento jurídico que devidamente utilizado pode impedir a utilização de tais dados, bem como responsabilizar o criminoso civil e penalmente.

Se assim fosse estaríamos justificando a prática de outro crime com base na legítima defesa, passando de vítima a criminoso. Existindo ainda o excesso na reação, excesso esse punível pela lei.

Nesse passo, trazemos à tona outra tese que justificaria tal medida: a inexigibilidade de conduta diversa, que consiste na possibilidade de

permitir que a vítima, nas circunstâncias em que ocorreu o fato, tivesse comportamento diferente que o permitido pela norma, agindo em desacordo com a lei.

Para elucidar, citamos o caso real da absolvição do jovem que cometeu homicídio causado por iminência de assalto. Ao dirigir em avenida perigosa, o motorista viu um veículo com indivíduos mal encarados, aproximando-se e emparelhando em seu carro, dando a entender que se tratava de assalto. Ao tentar escapar, acelerou, capotando e matando os passageiros. O Tribunal de Justiça do Rio Grande do Sul o absolveu com base na tese de inexigibilidade de conduta diversa, entendendo ser plenamente aceitável que em época de insegurança e violência tal conduta seja justificável para aceitar o acidente.

Porém esse raciocínio é fundamentado apenas na doutrina, não há previsão em lei (conceito de causa supralegal de exclusão de culpa), sendo um dos temas mais tensos dentro da dogmática penal.

Voltando para o nosso exemplo, a política da corporação suportaria tal risco? O gerenciamento de riscos jurídicos no âmbito corporativo é forte fator de competitividade no mercado, revidar à invasão de seus sistemas pode trazer grandes riscos legais.

Por fim, trazemos a tese que encontra respaldo no cerne do Direito, discutindo questões mais profundas. Na antiguidade, se duas pessoas brigassem em razão de dívida, o credor poderia tomar qualquer bem do devedor, sem que houvesse ilícito, agindo conforme o que denominamos de autotutela; na Roma antiga os devedores eram escravizados para sanarem suas dívidas. No decorrer dos séculos, e diante de inúmeras injustiças cometidas, consolidou-se a noção de Estado de Direito, com conflitos resolvidos por autoridade estatal e um sistema de justiça mais civilizado.

No Brasil a autotutela é vedada, sendo aceita em raríssimas exceções expressas em lei. E mais, a autotutela foi tipificada penalmente no art. 345 do CP, que a considera crime de exercício arbitrário das próprias razões (fazer justiça com as próprias mãos).

As teses aqui expostas refletirão nos regulamentos de segurança das empresas, ponderando que os administradores devem resguardar suas corporações, com o objetivo maior de evitar o impacto de riscos jurídicos, relevando ainda que o direito não é uma ciência exata, e muito peculiarmente vai se adaptando à nova realidade.

Chegamos então à cautelosa conclusão que nosso país tem ampla legislação cível e penal que adequadamente manejadas podem afastar a sensação de vulnerabilidade, agindo em conformidade com os aspectos legais, sem riscos tão elevados para as empresas, que na realidade são as grandes vítimas dos criminosos virtuais.

Renato Opice Blum

Advogado e economista; Coordenador do curso de MBA em Direito Eletrônico da Escola Paulista de Direito; Professor convidado da FGV, PUC/PR, IBMEC e outras; Árbitro da Câmara de Mediação e Arbitragem de São Paulo (FIESP).

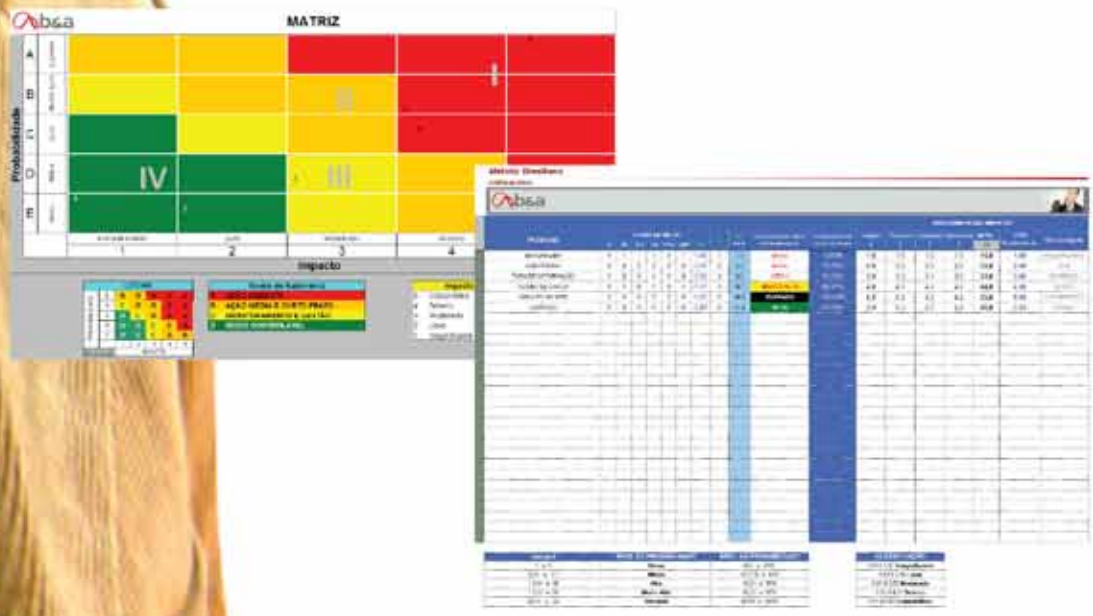
Camilla do Vale Jimene

Advogada; Professora do curso de pós-graduação em Direito Eletrônico da Unigran; Professora da UNIP.

sumário

FERRAMENTA de TI sua solução SOB MEDIDA

O sistema AudiXpress possibilita, de forma **integrada, agregar valor** e **facilitar** a operação e **controle** da Gestão de Riscos Corporativos da sua empresa.

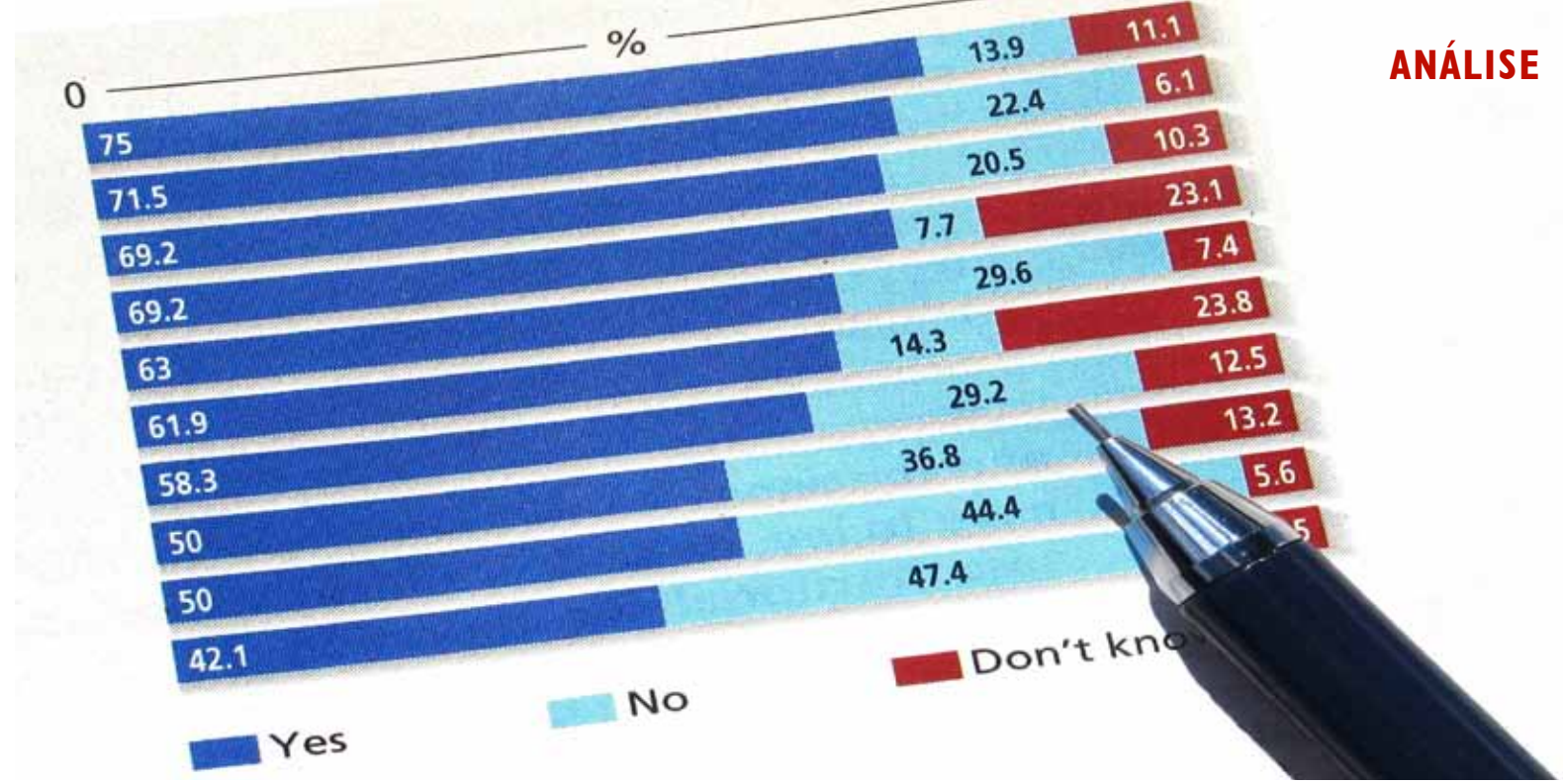


Benefícios:
– Otimização de recursos;
– 4 Módulos em UM, distintos, mas integrados: Auditoria Baseada em Riscos; Gestão de Riscos Investigação; Plano de Continuidade de Negócios

murah audiXpress

informações | www.brasiliano.com.br
| info@brasiliano.com.br

b&a BRASILIANO&ASSOCIADOS



A Importância da Realização de Testes do PCN: Fator Crítico de Sucesso

Rosângela Aparecida Stringher

O universo corporativo possui inúmeras necessidades que devem ser supridas constantemente. Entre elas está o desenvolvimento preventivo de um conjunto de estratégias e planos de ações, a fim de garantir que os serviços essenciais - frente à ocorrência de um evento de grande magnitude -, sejam devidamente identificados, preservados e, principalmente, mantidos operacionais. Isso, até que a situação se estabilize e o funcionamento da organização seja normalizado dentro de seu contexto de negócio, considerando duas variáveis essenciais: os componentes e os processos.

Para isso há o Plano de Continuidade de Negócios (PCN), também conhecido como Business Continuity Plan (BCP). Pesquisas realizadas em grandes organizações de diversos segmentos constataram que apenas 8% das organizações que não têm um PCN sobrevivem após um grande incidente (Safetynet/Guardian). Tais pesquisas revelaram que o risco mais temido pelas corporações é o de danos à reputação da empresa, seguido pelo de interrupção de negócios e em terceiro lugar pelo de responsabilidade civil, potencializado pela globalização (AON).

"O importante nos testes é executar os procedimentos previstos e torná-los de conhecimento do maior número de colaboradores, para que em possível situação de contingência, as ações necessárias e programadas sejam executadas naturalmente, sem transtornos. Um segundo produto que se obtém dos testes é a depuração do plano." (Antonio Celso Ribeiro Brasiliano).

A Brasiliano & Associados considera os testes de PCN um ponto de gargalo da Gestão de Continuidade de Negócio (GCN), por isso, desenvolve com sua metodologia e abordagem pró-ativa uma estratégia que permite de forma clara e prática a aplicabilidade dos mesmos, objetivando constatar se o plano de resposta da organização é factível.

A realização de testes no PCN é considerada um fator crítico de sucesso a medida que permite a verificação pela organização da exequibilidade do conteúdo do seu plano. Validar a operacionalidade das ações descritas por meio da realização de testes é condição essencial para que o plano não seja apenas um documento "para inglês ver" .

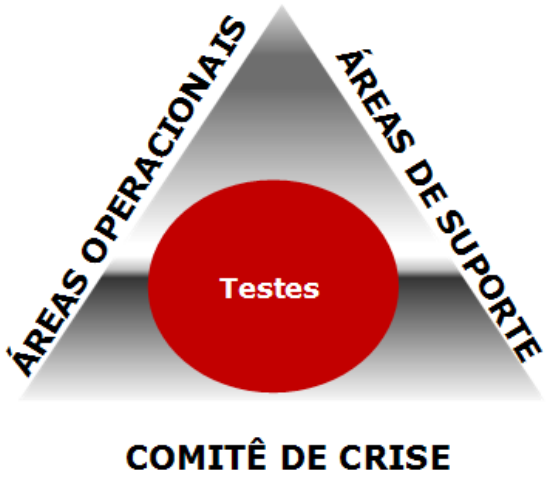
"O importante nos testes é executar os procedimentos previstos e torná-los de conhecimento do maior número de colaboradores, para que em possível situação de contingência, as ações necessárias e programadas sejam executadas naturalmente, sem transtornos. Um segundo produto que se obtém dos testes é a depuração do plano." (Antonio Celso Ribeiro Brasiliano).

Cabe ressaltar que para obter a certificação de sua GCN, uma organização deve atender aos quinze aspectos da norma ABNT NBR 15999-2. Dentre esses aspectos estão os testes, que deverão ser documentados, através de sua formalização e registro.

Os testes devem ser de conhecimento do maior número de colaboradores, para que as ações programadas sejam executadas naturalmente e sem transtornos frente a um evento inesperado.

Um plano de testes pode ser executado para um único procedimento operacional ou para um conjunto deles. Deve contemplar cenários e locais para execução e, principalmente, as atividades que deverão ser validadas por uma equipe de inspeção e acompanhamento durante a realização dos testes.

Os testes de PCN podem ser divididos para abranger as chamadas camadas estratégicas (Figura 1), que são: áreas operacionais, áreas suporte e comitê de gerenciamento de crise.



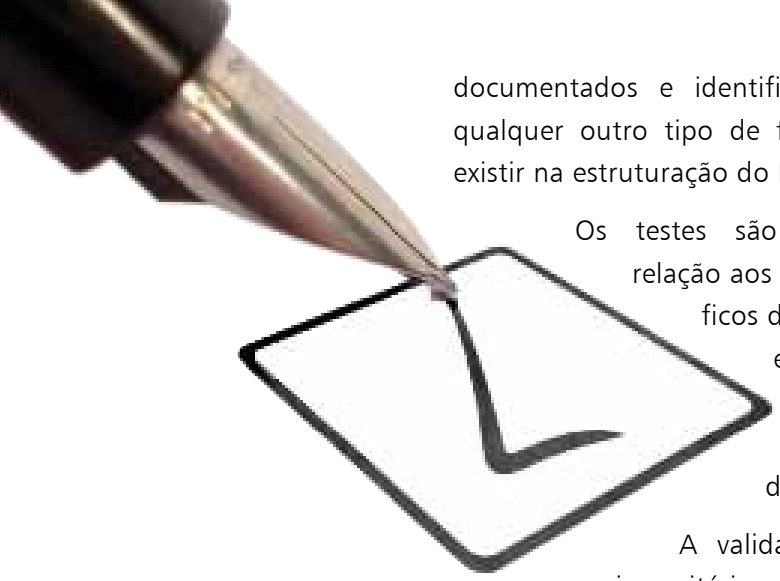
Figiura 1

PRIMEIRA CAMADA ESTRATÉGICA (Áreas Operacionais)

Diz respeito a sensibilização e conscientização dos gestores e colaboradores das áreas de negócio para que possam praticar seus processos críticos em situações anormais, em situações de contingência com efetivo reduzido – cerca de 30%.

SEGUNDA E TERCEIRA CAMADA ESTRATÉGICA (Áreas de Suporte e Comitê de Crise)

Diz respeito ao treinamento dos componentes do Grupo de Respostas a Contingência, ou seja, são as áreas responsáveis por dar suporte operacional no caso de uma contingência. Neste caso específico para a EMPRESA, esse grupo será o Comitê de Crise, tendo como integrantes as áreas de suporte. O objetivo deste tipo de teste é confirmar a adequação dos procedimentos



documentados e identificar lacunas ou qualquer outro tipo de falha que possa existir na estruturação do Plano.

Os testes são avaliados em relação aos objetivos específicos da infra-estrutura e aos procedimentos que os colaboradores devem executar.

A validação dos testes exige critérios de avaliação em alguns casos, como:

- posse dos aplicativos necessários;
- realização de seus processos críticos – operacionalização no tempo máximo de duas horas;
- conhecimento do PCN pelos colaboradores chave;
- ações do comitê de decisão;
- funcionamento dos equipamentos e da infra-estrutura;
- adequação do número de colaboradores para a execução dos processos críticos;
- desmobilização dos colaboradores;
- processos de comunicação (Início da situação, evolução de acontecimentos e no retorno a situação de normalidade).
- preparação do relatório (ações efetuadas, dificuldades e sugestões).

Embora haja um leque de modernos conceitos corporativos, muitas organizações se deparam com quatro mitos envolvendo a aplicabilidade dos testes, os quais são esclarecidos a seguir:

1º Diz respeito à idéia de que os testes são feitos para provar que o Plano funciona. Nesse caso, um teste que vier a expor erros será um teste falho. **Não existem testes falhos. Os testes devem ser realizados para, entre outros objetivos, identificar falhas.**

2º Diz respeito ao REALISMO. Para alguns profissionais um teste de PCN tem que reproduzir, do modo mais fiel possível, o ambiente de contingência e, para isso, deve-se chegar ao ponto de interromper as atividades do dia-a-dia para executá-lo. **Tal procedimento é desnecessário e contraria a essência do Plano de Continuidade que é garantir a continuidade das operações vitais.**

3º Diz respeito à TOTALIDADE. Este mito diz que um teste só é válido se todo o plano for testado. **A construção de um PCN é por módulo, portanto deverá ser testado por módulo. Essa estratégia é mais factível, viabilizando a realização de mais testes.**

4º Diz respeito à CAPACITAÇÃO. Toda empresa deve estar suficientemente preparada para enfrentar as contingências. **Uma empresa jamais estará preparada para enfrentar uma contingência. A não ser que "suficientemente preparada" signifique estar consciente das ações básicas necessárias. Fatores de Sucesso são: INTUIÇÃO, DEDICAÇÃO, EFETIVA PARTICIPAÇÃO E CAPACIDADE GERENCIAL. Tudo isso somado à capacidade técnica das equipes e do PCN.**

É importante lembrar que o processo da GCN, também conhecido por "ciclo de vida da continuidade de negócios", é retro-alimentativo e representa a operação de todo seu programa dentro da organização além de englobar o ciclo PDCA - o meio de garantir que a continuidade de negócios esteja gerenciada e aprimorada de forma eficaz - e se aplica a todas as partes do ciclo de vida da GCN. (Figura 2)

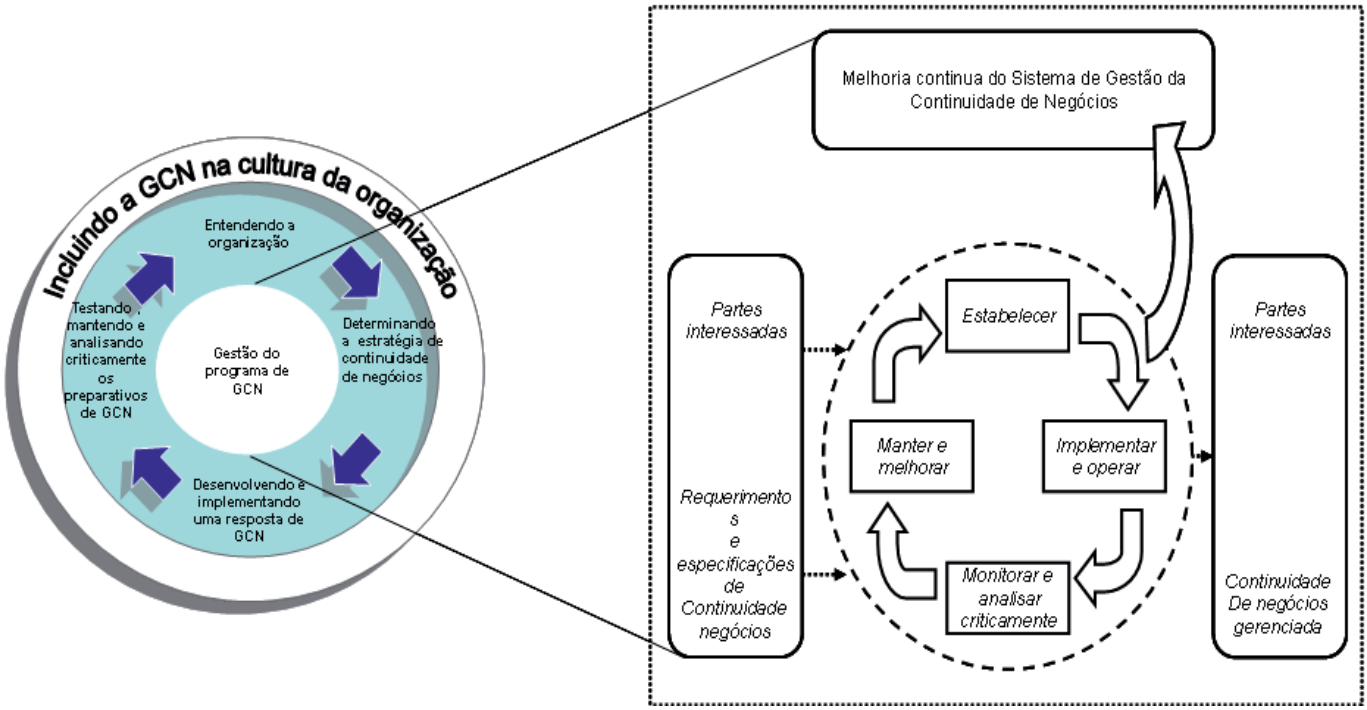


Figura 2

Um Plano de Continuidade de Negócios feito por especialistas embasados em conhecimentos técnicos é capaz de manter uma corporação inabalável frente às intempéries que possam ocorrer de toda e qualquer natureza. A realização de testes integra a prática de quem estabelece um processo para a realização do PCN e constitui-se num fator essencial para que o plano ocorra com êxito e mantenha o processo da GCN.

Rosângela Aparecida Stringher
Consultora da Brasiliano & Associados
rstringher@brasiliano.com.br

sumário

A Importância de um MBA na profissão de Gestor de Riscos

Álvaro Takei

O aprendizado não tem fim, principalmente para o profissional que quer se destacar como gestor (gerente, diretor ou presidente) de sucesso. A educação continuada é fundamental, especialmente quando se trata de atualização com foco em novas tecnologias, habilidades de comunicação e estratégias de desenvolvimento profissional e pessoal.

Obter esse desenvolvimento significa ter que escolher programas dentre uma infinidade dos que são oferecidos, atualmente, no mercado de treinamento e educacional. Podem ser cursos livres, que não exigem nenhum requisito anterior de formação e que, mesmo assim, podem auxiliar muito no exercício profissional.

Por outro lado, aos que possuem formação superior, os passos a serem dados depois da conclusão da graduação em uma faculdade ou universidade, devem ser: realizar um curso de pós-graduação, que pode ser na forma de curso de especialização ("*lato sensu*"), seguido de um mestrado acadêmico (tradicional) ou mestrado profissionalizante e, por último, um doutorado (estes últimos "*stricto sensu*").

A diferença entre os diversos cursos de pós-graduação, de forma resumida, está no conteúdo, carga horária e finalidade. Assim:

- Os **cursos de especialização "*lato sensu*"** visam especializar o participante em alguma área do saber. Ao final do curso, o aluno apresenta uma monografia ou trabalho de conclusão. A duração mínima é de 360 horas/aula e pode ser concluído em um ano ou em um ano e meio;
- Os **mestrados profissionalizantes** proporcionam a capacitação dos alunos para a produção de novas técnicas e processos no mercado. O trabalho final pode ser uma pesquisa, projeto ou análise de caso(s). A duração é geralmente superior a um ano e meio.

- O **mestrado acadêmico** foca a formação de professores universitários. O mestrando apresenta uma dissertação no final do curso, que dura, em média, de 2 a 3 anos;
- O **doutorado** é estruturado para formar pesquisadores, bem como para ampliar os conhecimentos dos professores universitários. É finalizado com a defesa de uma tese depois de um período de curso de quatro a cinco anos.

Existem ainda os chamados MBA's, que são, normalmente, cursos de administração direcionados a profissionais de diferentes formações que querem aprender a gerenciar negócios. Têm duração de 360 horas/aula ou mais e podem ser concluídos no período de um a dois anos

MBA é a sigla em inglês para "*Master in Business Administration*", a tradução literal significa Mestrado em Administração de Negócios. Basicamente, existem duas categorias de MBA's: os "*full-time*", que exigem dedicação integral e os "*part-time*", que permitem conciliar vida estudantil com trabalho. A maioria dos programas brasileiros são "*part-time*", havendo, inclusive, os que são oferecidos à distância.

Os MBA's surgiram, efetivamente, como uma forma de aprofundar os conhecimentos em Administração de forma geral. Entretanto, por necessidade dos interessados, foram sofrendo modificações no conteúdo, adquirindo um formato que permite a especialização um uma determinada área, uma delas a Gestão de Riscos.

A Gestão de Riscos vem, gradativamente, aumentando em importância nas organizações, a qual vem acompanhada de maior responsabilidade para os profissionais que atuam na área e, naturalmente, maior visibilidade. Por isso a aquisição de conhecimento para estes profissionais passa a ser crucial, e os que já possuem um curso de graduação, podem obtê-lo com a realização de um MBA em Gestão de Riscos.

Ao constatar a importância de um MBA para os profissionais de Gestão de Risco, fica um alerta para aqueles que ainda não possuem um diploma de curso superior: de que devem, urgentemente, sanar esse *gap* educacional, para que possam manter sua empregabilidade. Lembrando que hoje, o importante não é ter um emprego, mas ser "empregável".

Álvaro Takei
Diretor de Ensino Digital da Brasiliano & Associados
takei@brasiliano.com.br

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

DESAFIO AOS DEUSES: A FASCINANTE HISTÓRIA DO RISCO

Em uma narrativa que se assemelha a um romance, o autor acredita que o risco não precisa ser tão temido hoje: administrá-lo tornou-se sinônimo de desafio e oportunidade

Se você é totalmente fascinado pelo tema de análise e gestão de riscos, nunca é tarde para uma imersão no livro "Desafio aos Deuses - A fascinante história do risco" (Campus/Eselvier), escrito pelo americano Peter Lewyn Bernstein. Para aqueles que se familiarizam com a gestão de riscos e desejam entender um pouco mais sobre como o risco tem sido tratado historicamente este livro é obrigatório.

Bernstein foi um historiador financeiro, economista e educador que ao desenvolver e refinar a teoria dos mercados eficientes (*efficient market theory*), tornou-se uma das maiores autoridades em popularizar e apresentar investimentos econômicos ao público comum.

A obra discorre de maneira cronológica a história do risco, versando também sobre a importância da indústria de seguros, dos bancos e da indústria de Venture Capital no desenvolvimento e avanço da Civilização.

Na obra, o autor faz uma restrospectiva histórica bastante informal, é verdade, de como a mente humana procurou abordar as incertezas e riscos associados ao futuro desde a civilização helênica até os dias atuais, relatando como a humanidade se libertou dos oráculos e adivinhos, mediante as ferramentas poderosas da administração do risco disponíveis nos dias de hoje.

Trata-se de um relato histórico com uma fluidez literária raramente vista, que narra a forma como o Homem conseguiu, com o passar dos anos, traduzir em números os fenômenos antes considerados puro acaso. A narrativa aborda de modo leve temas como seguros, derivativos e teoria dos jogos. Tudo tendo o risco como pano de fundo.

O título é a tradução literal do inglês "Against the Gods" (trocadilho com "against the odds") que remete a uma das passagens iniciais dessa história. Até a Renascença Italiana os jogos de azar não levavam em conta o conceito de probabilidades, e por exemplo em um jogo de dois dados se apostava por um resultado 6 a mesma quantia que por um 2 ou um 12. Parece absurdo para nós, mas na concepção da época o resultado dos dados era considerado uma vontade de Deus, e não poderia haver regras que governassem essa vontade.

Foi Girolamo Cardano, um inveterado jogador, matemático e também o médico mais famoso da sua época, que escreveu o tratado *Liber de ludo aleae* (Livro dos jogos de azar) onde pela primeira vez se desenvolveu os princípios estatísticos da probabilidade, o que além de lhe proporcionar grandes lucros mudou para sempre a forma como vemos os acontecimentos futuros.

Existe um grau de ordem mesmo em um futuro incerto, e conhecê-lo permite que possamos nos preparar para ele.

Bernstein acompanha não só o desenvolvimento da matemática por trás da probabilidade, com Pascal, Fermat e os Bernoulli, mas também como isso impactou a sociedade da época. Conta como o trabalho de John Graunt acompanhando os nascimentos e óbitos de Londres deu origem ao moderno cálculo atuarial. Podemos ver o surgimento do Lloyd's em uma taverna inglesa de mesmo nome, onde eram postadas notícias das chegadas e partidas dos barcos e se negociavam os lucros e prejuizos futuros com a carga. E conhecer Francis Galton, o homem que media tudo, que se tornou simultaneamente o pai da eugenia e da distribuição normal, que introduziu o conceito vital de "regressão à média".

A última parte do livro trata do risco no século XX, em especial do trabalho de John von Neumann com a teoria dos jogos. Para mim essa é o assunto mais fascinante: independente da matemática do risco, tão ou mais importante é como nós reagimos a ele. Ou seja, voltando a missão da Segurança Corporativa, quando um risco é ou não aceitável? Bernstein explica maravilhosamente todas as implicações do comportamento humano na nossa relação com o futuro.

A idéia central do livro é que risco não significa perigo. Significa simplesmente não sabermos o que o futuro nos reserva. Bernstein, que fez carreira como gestor de investimentos, professor (inclusive em Harvard) e autor de vários livros, morreu no último dia 5 de junho de 2009 de pneumonia.

Acima de tudo, "Desafio aos Deuses" é um livro incrivelmente bem escrito, fácil e divertido de ler. Nenhuma base matemática é necessária, e o autor introduz as diversas noções de probabilidade e risco a medida em que a humanidade as foi descobrindo. Leitura obrigatória para qualquer profissional. A obra ganhou o prêmio FinancialTime/Booz-Allen & Hamilton - livro de negócios mais inovador/96.

RISCO "E OPORTUNIDADE" DIGITAL

Até abril de 2006 a Internet contava com mais de 1 bilhão de usuários, quase a mesma quantidade de usuários de aparelhos celulares no mundo todo. Esses números assustam quando pensamos na quantidade de pessoas que têm acesso às informações da rede, o que nos causa uma grande insegurança.

Em "Risco Digital", o autor, Leonardo Scudere, diretor da Unidade de Negócios de Segurança da CA, Inc. para América Latina e presidente do Capítulo Brasil da HTCIA, trata das principais questões relacionadas a risco digital, com uma abordagem voltada para o público leigo de executivos e para o público em geral. O objetivo da obra é levar o leitor a perceber como o novo meio digital possibilita uma reconfiguração social e a identificar possíveis danos que esse meio pode causar, a fim de enfrentar com maior sabedoria os desafios que, em grande parte, transcorrerão nesses novos domínios digitais.

Com linguagem não técnica, o autor usa exemplos práticos do cotidiano, na tentativa de aproximar leitores que não lidem com o assunto, levando informações mais voltadas a empresas e assuntos como riscos de contenção, segurança,

inteligência e geração de valor corporativo. No livro ainda são citadas pesquisas sobre um levantamento feito pelo FBI em janeiro, que revela quem são os verdadeiros crimonosos na internet, os quais causaram prejuízos diretos de R$ 67 bilhões à empresas americanas.

Scudere não se limita aos serviços via web. Avalia também a segurança nos celulares, aparelhos de mp3, cartões de crédito, a chegada do Blackberry. Explica que seu foco "é conquistar a atenção dos executivos e do público em geral, os quais, à exceção do estritamente necessário, não irão ver, nessas idéias, desnecessárias estatísticas. A intenção é promover uma reflexão acerca dos desafios que nos cercam, já que grande parte de nossa vida transcorrerá nesses novos e, por vezes, obscuros domínios digitais".

Como a tecnologia pode agregar valor aos negócios

O autor acredita que a tecnologia pode ser uma aliada para o crescimento dos negócios, criação de novas oportunidades e redução das fraudes. Seu objetivo é desmistificar os "perigos" da internet e mostrar as vantagens competitivas que esta parceria traz, sempre analisando os conflitos sociais.

Difícil de entender? Não. Scudere abre mão dos termos técnicos e recorre a exemplos práticos do cotidiano, aproximando o leitor e estreitando sua relação com o tema. Os ataques contra policiais ocorridos este ano na cidade de São Paulo, ilustram bem a idéia do autor. Na ocasião, o desfecho das articulações dos mentores foi a paralisação dos serviços de comunicação via celular e lentidão e interrupção na internet.

"Quero convidá-lo a uma reflexão conjunta e madura sobre esse momento e transmitir minhas preocupações sobre cenários e incidentes tão semelhantes e com os quais estou diariamente envolvido no mundo cibernético. Não será tarefa simples porque talvez nunca ocorra imagem ao vivo tão tangível como as que comento, além de várias que ocorreram após as datas mencionadas, que me permita explicar as conseqüências igualmente danosas desses atos", explica Scudere.

A proposta do autor é esclarecer e reforçar a importância das empresas levarem em consideração os riscos de contenção, segurança, inteligência, e geração de valor corporativo, chamados de "digitais". Essa relevância aumenta quando o assunto tratado é o setor bancário, que movimenta hoje cerca de R$ 6 bilhões em transações online e de R$ 27,8 bilhões em canais eletrônicos no geral. Como evitar ou minimizar os riscos?

Quais são os reais inimigos cibernéticos? Scudere cita na obra um levantamento feito pelo FBI em janeiro. A pesquisa divulgou que os ataques cibernéticos custaram R$ 67 bilhões em prejuízos diretos às empresas americanas em 2005. Conseqüentemente, o FBI colocou como terceira principal prioridade para 2006 a proteção contra ataques e delitos utilizando alta tecnologia computacional. "Existe um consenso de que não houve avanços significativos em praticamente nenhuma das áreas-foco, mesmo aquelas mais visíveis, como a segurança dos aeroportos", analisa.

Risco Digital propõe ao leitor uma reflexão sobre os benefícios profissionais e pessoais que o ambiente digital possibilita e sugere modelos que podem proteger você de ameaças e impactos, talvez ainda não percebidos. Oferece também uma visão sobre as preocupações dessa dinâmica, articulando possíveis caminhos na constante busca do equilíbrio ideal entre risco e oportunidade nos desafiadores domínios digitais.