

**4** O uso de dispositivos  
móveis nas empresas

**9** A ferramenta BIA  
*Business Impact Analysis*

**2** ponto de vista  
Filosofia em tempos  
de desgovernança

**12** Seminário Gestão de Riscos  
Corporativos para EFPC

**13** Roubo de cargas: desafio para  
empresas e autoridades

**16** Cenários prospectivos e a  
economia brasileira

**19** A segurança corporativa na  
estratégia dos negócios

**22** Cursos Brasileiro & Associados  
em agosto e setembro

**23** Amplie seus conhecimentos  
com a biblioteca Sicurezza

## Filosofia em tempos de

# desgovernança

**Os livros de filosofia raramente são concebidos em um ponto preciso do tempo ou em algum lugar específico. Kant escreveu *A Crítica da Razão Pura* durante 11 anos.**

**Spinoza trabalhou a maior parte da sua vida em *A Ética*. Sócrates jamais escreveu uma única linha.**

**Este editorial, hoje, é diferente de anteriores, pois a ideia foi concebida quando o Brasil vive tempos de “desgovernança” como nunca antes. Vivemos os desfechos da operação Lava Jato, com envolvimento de megaempresários, políticos do alto escalão e ex-executivos da estatal Petrobrás.**



**Antonio Celso Ribeiro Brasiliano**  
CRMA, CES, DEA, DSE, MBS

*Publisher da revista Gestão de Riscos,  
diretor-presidente da Brasiliano & Associados  
brasiliano@brasiliano.com.br*

*Teriam nossas leis clássicas se tornado obsoletas diante das novas ameaças? Quem é soberano de quem? Será o diálogo uma prática cultural específica que, às vezes, pode simplesmente se mostrar inadequada? E, mais importante, sob que condições o diálogo é uma opção viável?*

*Trata-se ainda de uma questão aberta: saber se essa “desgovernança” pode ser prática terrorista, se esse terrorismo pode ser distinguido de uma guerra e, finalmente, se o Estado brasileiro pode declarar guerra a algo que não seja uma entidade política – a falta de ética e a queda de seus valores morais.*

*A batalha contra esta “desgovernança” não é uma simples partida de xadrez. Não existem regras pré-estabelecidas, não há distinção entre lances legítimos e ilegítimos.*

*A filosofia começou a avaliar se a razão poderia ter responsabilidade moral e social intrínseca e, com base nisso, se a filosofia deveria desenvolver uma relação mais ativa com situações como essa que estamos vivendo: de “desgovernança”.*

*Para Kant e outros filósofos do Iluminismo, tornou-se claro que a autoafirmação da razão tem impacto histórico, pois só a razão é capaz de indicar como transformar o presente em futuro melhor. Dessa forma, a nossa liberdade é medida pelo grau*

*em que nos tornamos aptos a adquirir controle sobre os fatores de riscos dessa situação, pois de outro modo ela nos controlaria.*

*A ideologia explícita dessa “desgovernança” e de seus fatores de riscos é uma rejeição à modernidade, que na filosofia está associada ao conceito do Iluminismo no século 18 e marca uma ruptura com o passado. Ela só é possível com base na independência do indivíduo diante do totalitarismo (união do poder político e religioso), independência que é a marca da modernidade!*

*Hoje, quando perguntamos se vivemos em uma era iluminada, a resposta é não. Vivemos em uma era de iluminação. Kant estava certo ao lembrar que nunca podemos confiar estarmos em uma era iluminada, mas em uma era na qual a iluminação é um processo que tem necessidade constante de ser cultivado. Kant entendia que a modernidade é uma mudança na atitude de crença, no modo como acreditamos mais do que naquilo em que acreditamos.*

*É isso que precisamos fazer: mudar nossas crenças, agir, tomar atitudes. Só assim poderemos controlar os fatores de riscos dessa “desgovernança” que hoje se espalha pelo Brasil em velocidade patológica.*



# Dispositivos móveis pessoais e a segurança

# da informação

***O avanço das tecnologias aplicadas nos dispositivos móveis e a quantidade de smartphones, tablets e notebooks adquiridos pelo consumidor estão permitindo que uma tendência se torne realidade: a utilização de dispositivos móveis pessoais para desenvolver atividades de trabalho.***

Essa tendência, chamada BYOD – Bring Your Own Device (“traga seu próprio dispositivo”), tem se tornado cada vez mais frequente nas organizações e quando aplicada sob diretrizes pré-estabelecidas pode gerar benefícios como a diminuição de despesas com ativos, mas quando implantada sem uma análise prévia de riscos pode fragilizar a segurança das informações da empresa.

O conceito BYOD permite que colaboradores da empresa trabalhem a partir da utilização de seus próprios dispositivos, o que agrega valor no aumento da produtividade dos funcionários e consequentemente na melhoria da performance da empresa, além de diminuir gastos com ativos. É importante destacar a necessidade de um estudo do emprego do BYOD no ambiente corporativo seguindo as diretrizes e melhores práticas da área de segurança da informação, pois a falta de monitoramento dos dispositivos móveis conectados à rede pode acarretar em perdas inestimáveis para a empresa.

Por isso, antes de entrar de cabeça nessa tendência as empresas devem elaborar um estudo de análise de riscos para identificar possíveis fragilidades, evitando a exposição a riscos que possam impactar negativamente sua reputação perante o mercado. Esses estudos podem ser elaborados com base em normas como a ISO 31000 - Gestão de Riscos Corporativos, que fornece as melhores práticas para identificação de riscos, e a ISO 31010, que especifica 28 técnicas para sua gestão. A utilização de metodologias com critérios pré-estabelecidos em acordo com as normas técnicas pode auxiliar os gestores a analisar, avaliar e tratar de maneira preventiva os riscos ligados à implantação do BYOD.

## Pesquisas mostram abrangência do tema

A MDM Solutions, empresa especializada em soluções de gerenciamento e mobilidade corporativa apresentou em 2015 a pesquisa “BYOD no Brasil: Adoção, Gestão e Desafios na Visão dos Líderes de TI”, para a qual foram entrevistadas 73 empresas, 34% delas com faturamento superior a R\$ 1 bilhão. Os resultados mostraram que 70% das entrevistadas planejam investir na área nos próximos 12 meses. A IDC, empresa de consultoria e pesquisa de mercado, aponta que 480 milhões de smartphones estarão em utilização em 2016 e 65% destes serão utilizados para BYOD. Já o Gartner Inc. estima que, em 2018, 70% dos colaboradores de empresas em todo o mundo estarão utilizando seus dispositivos móveis para atividades de trabalho.

As práticas de BYOD podem gerar oportunidades para alavancar negócios e diminuir gastos operacionais, mas também apresentam riscos relacionados aos dados corporativos. Algumas vantagens podem ser vistas com relação ao custo benefício da implantação, como no caso de empresas que contam com equipes formadas por diversos colaboradores que necessitam de dispositivos móveis para execução de trabalhos externos. Ao

invés de comprar notebooks ou tablets para todos os colaboradores, o conceito permite que eles utilizem seus dispositivos pessoais.

Além da economia na aquisição de ativos e manutenções, outro ponto positivo é a familiarização dos colaboradores com seus próprios dispositivos móveis. Colaboradores que utilizam seus smartphones, tablets ou notebooks, já conhecem os sistemas operacionais, aplicativos, atalhos e principais funcionalidades, diminuindo os gastos da empresa com treinamentos extensivos. Mais do que isso, existe a possibilidade de os dispositivos móveis dos colaboradores possuírem tecnologia mais avançada que aqueles oferecidos pela empresa.

Apesar dos diversos benefícios da solução, a utilização de BYOD nas empresas pode esconder alguns riscos que afetam diretamente e negativamente a sua produtividade e os seus objetivos estratégicos. Da mesma forma que a empresa pode economizar, possivelmente terá de aumentar o investimento em segurança. Não realizar o gerenciamento adequado dos dispositivos móveis conectados à rede corporativa pode facilitar a ocorrência de diversos riscos ligados à segurança da informação.

Uma pesquisa realizada pela Kaspersky em conjunto com a B2B Research revelou que 18% entre as empresas entrevistadas sofreram vazamentos de dados confidenciais através de dispositivos móveis pessoais dos colaboradores. No estudo realizado pela MDM Solutions, um número aponta diretamente para o quesito segurança: 30% das empresas entrevistadas permitiam que os funcionários utilizassem seus dispositivos móveis na rede corporativa sem a implantação de políticas ou ferramentas para monitoramento desses dispositivos.

## Necessidade de análise dos riscos

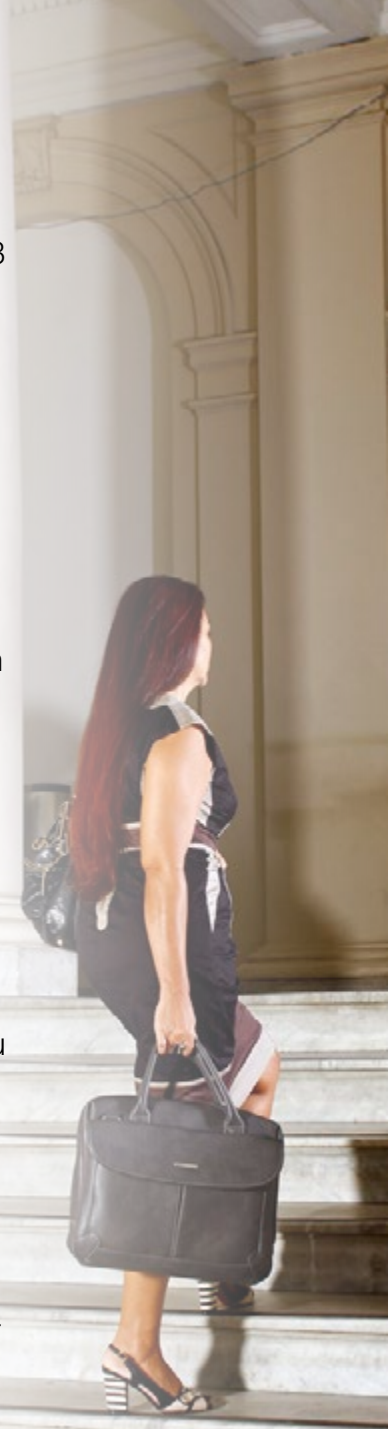
A empresa Navita, de mobilidade corporativa, realizou pesquisa em 2013 com 204 líderes de empresas de tecnologia da informação que mostrou alguns números associados aos riscos do BYOD: 71% das empresas possuíam histórico de pelo menos um caso de roubo ou furto de equipamentos com dados corporativos; 44% tiveram ocorrências por falta de criptografia dos dados; 44% tiveram problemas com senha; 19% não possuíam backup dos dados e 18% relataram problemas com dados pessoais que se tornaram públicos.

Outro dado preocupante quando falamos de dispositivos móveis é o crescimento de malwares. O primeiro malware ou software malicioso descoberto em dispositivos móveis foi batizado com o nome de Cabir, em 2004. O vírus contaminava e se espalhava por celulares que utilizavam o sistema operacional Simbyam da NOKIA através de conexão Bluetooth. Hoje, 11 anos depois, o aumento dos vírus que atingem dispositivos móveis foi gradativo. No relatório expedido em 2015 pela

McAfee, dedicada à tecnologia de segurança, o volume de malwares para dispositivos móveis em seu laboratório, que no último trimestre de 2013 ultrapassava a marca de 3 milhões, teve o número dobrado no mesmo período de 2014, ultrapassando 6 milhões. A América do Sul possui taxa de 7% de infecção.

Da mesma forma que o número de malwares cresce exponencialmente, os ataques cibernéticos direcionados também tendem a aumentar. Uma das operações mais famosas foi a “outubro vermelho”, descoberta em outubro de 2012. A operação era dirigida a órgãos diplomáticos e governamentais em todo o mundo, inclusive no Brasil. Os ataques tinham a finalidade de desviar dados de inteligência, infectar sistemas, redes empresariais e dispositivos móveis pessoais. Cada vez mais dispositivos móveis serão alvos de ataques para acessar informações confidenciais armazenadas em servidores ou banco de dados corporativos.

Olhando para o histórico de incidentes ligados a segurança da informação, como aplicar a gestão de riscos para o uso dos dispositivos móveis no ambiente organizacional? Segundo a norma ISO 31000, a gestão de riscos é “um conjunto de atividades conduzidas em uma organização que visam





dirigir e controlar seus riscos”. Essas atividades possibilitam que as organizações criem indicadores para avaliar seu cenário atual, medir os riscos, verificar a eficácia de seus controles e traçar estratégias para o tratamento de seus riscos.

Para que o gerenciamento dos riscos ocorra de maneira eficaz nas organizações existem metodologias apoiadas em normas nacionais e internacionais que, aplicadas de maneira sistêmica permitem identificar quais são os riscos que podem impactar negativamente sua imagem, facilitando as tomadas de decisão.

O Método Brasileiro de Análise de Riscos Corporativos fornece um processo para identificação, análise e avaliação dos riscos e utiliza o framework da norma ISO 31000 como estrutura principal, o que permite ser aplicado a qualquer estrutura empresarial ou segmento de mercado. O método tem em seu framework ferramentas práticas e objetivas da norma ISO 31010, que fornece 28 técnicas para o processo de gestão de riscos. Outras normas podem utilizar essa estrutura para visão de alto nível do processo de gestão de riscos. A ISO 27005, por exemplo, fornece princípios e diretrizes para o processo de gestão de riscos de segurança da informação e utiliza como base o framework da ISO 31000.

Essa estrutura permite que o método possua não apenas um processo estruturado de gestão de riscos, mas também critérios pré-estabelecidos para analisar e avaliar os riscos ligados a BYOD identificados na empresa. Além das normas ISO 31000 e ISO 31010 o Método Brasileiro também utiliza o conceito da estrutura COSO - Committee of Sponsoring Organizations of the Treadway Commission, permitindo avaliar a

eficácia dos controles existentes nos processos de segurança da informação.

Segundo Brasileiro, “as empresas devem estar comprometidas com seus clientes, acionistas, parceiros comerciais e com a sociedade em que atua, focando esforços em reduzir os riscos existentes”, o que ratifica a importância da gestão de riscos nas organizações que pretendem utilizar ou já utilizam o conceito de BYOD.

O importante, independente do framework, métricas ou boas práticas escolhidas, é elaborar uma análise de riscos corporativos para o conceito BYOD, permitindo que sua empresa se proteja de riscos provenientes dessa solução e que possam impactar negativamente sua reputação.



**Alfredo Zanella**  
**CES, C31000, MBS**

*Bacharel em Sistemas de Informação,  
gerente da divisão de Consultoria  
e Tecnologia da Informação  
da Brasileiro & Associados  
alfredo@brasiliano.com.br*

# Inteligência em **riscos corporativos**

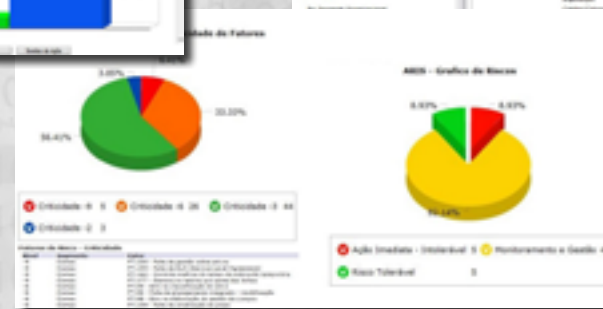
SOFTWARE **GRC BM**

*As disciplinas de risco integradas  
para interpretação de informações*

DASHBOARD EXECUTIVO  
COM RELATÓRIOS  
INSTANTÂNEOS PARA  
ANÁLISES ESTRATÉGICAS



CUSTOMIZAÇÃO  
PARA CADA  
PERFIL DE NEGÓCIO



**TODAS AS FERRAMENTAS DE GESTÃO DE RISCOS**

COM BASE NA ISO 31000 E COSO I E II - FRAMEWORK DO MÉTODO BRASILEANO



**GESTÃO DE RISCOS  
CORPORATIVOS**  
BRASILIANO E MINICOM

SOFTWARE



11 5531 6171  
[www.brasiliano.com.br](http://www.brasiliano.com.br)



# A ferramenta BIA na estratégia dos negócios

***O planejamento estratégico tem por objetivo direcionar os rumos de um negócio. É um processo contínuo e sistemático, cujo monitoramento e controle dos processos são essenciais para o cumprimento das metas e dos resultados futuros. Tomar decisões que envolvem riscos, organizar as ações necessárias para boa execução das decisões, retroalimentar e medir os efeitos dessas decisões são as principais tarefas.***

O planejamento estratégico é o processo de analisar uma organização sob diversos ângulos, direcionando seus rumos e monitorando suas ações de forma concreta. Dessa forma, para analisar o impacto de um processo, área ou unidade no negócio da empresa em caso de eventos futuros e o tempo de tolerância dos riscos utilizamos a ferramenta BIA – BUSINESS IMPACT ANALYSIS.

O uso dessa ferramenta, no caso de uma rede bancária, podemos analisar quais são as agências mais críticas para o negócio, aquelas que em caso de paralisação terão maior impacto para a empresa. Ou identificar quais são os processos críticos, para os quais a alta administração aplicará maiores recursos buscando minimizar os impactos no caso de ocorrer alguma paralisação.

Para que sejam alcançados os objetivos estratégicos, toda organização precisa que seus processos, atividades e áreas críticas não sejam prejudicados em caso de eventos futuros e para isso a ferramenta BIA utiliza dois critérios de avaliação: impacto no negócio versus tempo de tolerância.

O Método Brasileiro de Análise de Riscos define os critérios a serem aplicados para o impacto no negócio, divididos em quatro subcritérios com pesos diferenciados: imagem, financeiro, legal e operacional. Cabe aos gestores definir o peso de cada um, considerando seu nível de importância no contexto dos negócios da empresa. Por exemplo, para uma empresa de entretenimento infantil o maior bem,

intangível, é sua imagem, que deverá ter o peso. Para empresas que são dependentes de fluxo de caixa, o peso da imagem poderá ser menor e o peso financeiro maior, pois impacta diretamente na artéria da empresa.

Veja exemplo da aplicação do Método Brasileiro com o uso

**QUADRO 1**



IMAGEM		FINANCEIRO	
Critério	Pontuação	Critério	Pontuação
De Caráter Nacional - Brasil	05	Massivo - Acima de R\$ 500.000,00	05
De Caráter Regional	04	Severo - Até R\$ 500.000,00	04
De Caráter Local	03	Moderado - Até R\$ 100.000,00	03
De Caráter Interno - Dentro da Empresa	02	Leve - Até R\$ 25.000,00	02
De Caráter Interno - Dentro da Área	01	Insignificante - Até 5.000,00	01

LEGAL		OPERACIONAL	
Critério	Pontuação	Critério	Pontuação
Perturbações Muito Graves	05	Perturbações Muito Graves (impacta outros processos muito fortemente).	05
Graves	04	Graves (impacta outros processos de forma direta) e/ou Ocorrem impactos severos no abastecimento - clientes não atendidos.	04
Limitada	03	Limitadas (não impacta outros processos) e/ou Ocorrem impactos moderados no abastecimento - clientes não atendidos.	03
Leve	02	Leves (Impacta somente o próprio processo levemente) e/ou Ocorrem impactos leves no abastecimento - clientes não atendidos.	02
Muito Leve	01	Muito Leves (não impacta nada) e/ou Não há impacto no abastecimento - clientes não atendidos.	01

**QUADRO 2**

Grau de Impacto	Escala	Nível de Impacto
4,51 - 5,00	5	Massivo
3,51 - 4,50	4	Severo
2,51 - 3,50	3	Moderado
1,51 - 2,50	2	Leve
1,00 - 1,50	1	Insignificante

da ferramenta BIA no quadro 1. O nível de impacto é o resultado da multiplicação do peso pela pontuação de cada fator de impacto, depois dividido pela soma dos pesos. O resultado do nível de impacto é mostrado no quadro 2.

No nível de tolerância de tempo, como parte da avaliação do BIA, estima-se por quanto tempo o processo ou área analisada pelo gestor pode ficar indisponível ou inoperante sem que o *business* da empresa fique prejudicado. O importante é avaliar o tempo necessário para que o processo volte a ser operacional, mesmo que em condições precárias. O Método Brasileiro possui uma escala de valores de seis níveis, visando escalonar a criticidade de indisponibilidade de cada processo ou atividade, como mostra o quadro 3.

**QUADRO 3**

Tempo em Horas	Níveis de Tolerância
Até 4 horas	6
Até 1 Dia - 24 horas	5
Até 2 Dias - 48 horas	4
Até 7 Dias - 168 horas	3
Até 14 Dias - 336 horas	2
Mais de 14 Dias - 336 horas	1

**QUADRO 4**



quadrante laranja estão os MODERADOS, aqueles que ficarão em segundo plano e têm maior tempo de tolerância. No quadrante verde, os LEVES, que estarão no último plano para investimentos porque, independentemente do seu tempo de retomada, causam baixo impacto para o negócio.

É de fundamental importância que os gestores conheçam as estratégias de negócios da empresa para que a aplicação da ferramenta BIA permita identificar quais são seus processos, unidades e áreas que devem receber investimentos e atenção prioritária de seus administradores. Isso garantirá o êxito de continuidade dos negócios da empresa.

É comum vermos gestores elevarem o impacto de suas áreas no preenchimento do BIA por acreditarem que seus processos ou áreas são de fundamental importância para a organização. Para o resultado final da avaliação essa prática é perigosa, pois a alta administração investirá recursos, como tempo e dinheiro, de forma equivocada por conta da avaliação errônea de seus gestores.

O resultado do cruzamento do nível de impacto com o nível de tolerância de tempo é mostrado por uma matriz que define o nível de criticidade de cada processo e determina se ele é crítico, moderado ou leve, conforme exemplo no quadro 4.

Os processos considerados CRÍTICOS estão localizados no quadrante vermelho e exigem esforços para que não sejam paralisados em caso de eventos de grande magnitude, pois possuem curto tempo de tolerância e elevado impacto no negócio. No



**Talitha Medrado**  
CES, MBS

Consultora da Brasiliano & Associados, MBA em Gestão de Riscos Corporativos  
[talitha@brasiliano.com.br](mailto:talitha@brasiliano.com.br)



# seminário

## Gestão de riscos para operadores da Previdência

Gerenciar os riscos corporativos em uma EFPC, dimensionar os de maior relevância e determinar os controles necessários com o objetivo de entender a interconectividade entre os riscos de uma EFPC. O seminário organizado pela Brasiliano & Associados apresentará aos gestores ferramentas que permitem responder com técnica às diversas exigências dos planos de gestão, com base em práticas e regulações específicas para o setor.

No programa, além da análise conjuntural dos benefícios da gestão de riscos em nível nacional e mundial, as principais normas regulatórias (COSO I e II, ISO 31000 e 31010) e a resolução CGPC nº 13, de 1º de outubro de 2004, que exige a adoção de princípios, regras e práticas de governança, gestão e controles internos adequados ao porte, complexidade e riscos inerentes aos planos de benefícios e prevê que todos os riscos que possam comprometer os objetivos da EFPC sejam continuamente identificados, avaliados, controlados e monitorados.

Os participantes conhecerão o Método Brasileiro Avançado, que engloba: comunicação e consulta, contexto estratégico (política e processo de gestão de riscos, objetivos estratégicos), iden-

***A Brasiliano & Associados realiza, no próximo dia 19 de agosto, o seminário GESTÃO DE RISCOS PARA ENTIDADES FECHADAS DE PREVIDÊNCIA COMPLEMENTAR (EFPC), integrando controles internos e compliance***

tificação de riscos (emprego da ferramenta BIA para identificar processos críticos), mapeamento de processos, identificação de controles, diagrama de causa e efeito, emprego da matriz Swot para riscos, emprego da matriz de impactos cruzados, análise e avaliação dos riscos inerentes e residuais, tratamento dos riscos, ferramenta de priorização dos riscos e das ações, plano de ação e projeção futura, monitoramento, elaboração de indicadores de nível de criticidade dos riscos e dos riscos dos processos, implantação do plano de ação e eficácia das ações (BIA x Nível de Criticidade de Riscos x Nível de Riscos de Processos).

Também será apresentado o software GRC-BM, a principal ferramenta do mercado para gestão de riscos corporativos, que integra informações de todas as áreas da empresa, cruza dados e traça indicadores importantíssimos para tomada de decisões estratégicas. O seminário será apresentado pelo prof. dr. Antonio Celso Ribeiro Brasiliano (CRMA, CES, DEA, DSE, MBS), diretor-presidente da Brasiliano & Associados e acontecerá no próximo dia 19 de agosto no auditório da FAPI (av. 9 de Julho, 5.520, Jardim Europa, São Paulo). Informações: [www.brasiliano.com.br](http://www.brasiliano.com.br).

# Roubo de cargas: desafio para empresas e autoridades

***O primeiro trimestre de 2015 apresentou, em números absolutos, a maior quantidade de roubo de cargas no Estado de São Paulo dos últimos 10 anos, segundo dados da Secretaria de Segurança Pública; foram 2.372 casos e 62,3% (1.478) ocorreram na capital. Comparado a 2014, o aumento foi de 9,4%, mas na cidade de São Paulo o índice ultrapassou 17%.***

Comparados com os números de 2013, o crescimento do roubo de cargas no Estado de São Paulo foi de 29,6%, chegando a 36,4% na capital. Apesar da tendência de elevação ano a ano, se voltarmos a 2005, ano em que os dados começaram a ser divulgados, a evolução fica na casa dos 50%, tanto no Estado quanto na capital.

Esses dados mostram um problema complexo em razão de sua abrangência. Em 2014 foram registrados 8510 casos de roubo de cargas no Estado, implicando em prejuízos milionários para o setor. Números frios podem não revelar a gravidade do problema. Para se ter ideia, apenas na cidade de São Paulo foram registradas, no primeiro trimestre deste ano, média de 16 ocorrências por dia.

A Associação Nacional do Transporte de Cargas e Logística revelou, no XV Seminário de Transporte Rodoviário de Cargas realizado em abril, em Brasília, que os prejuízos no setor já ultrapassam R\$ 2 bi por ano, somadas as ocorrências de todo o país.

O gerenciamento de riscos é, portanto, vital para que as empresas entendam e administrem esse quadro, pela adoção de sistemática operacional e tecnológica para reduzir os riscos inerentes ao transporte. O roubo de cargas, como vimos, é um problema que no decorrer dos anos vem se agravando cada vez mais, sem perspectiva de reversão pelo menos pelos próximos anos e capaz de impactar negativamente no negócio do transporte de cargas.

O gerenciamento de riscos constitui-se numa forma de criar

recursos sem precedentes aos clientes. As empresas que mais bem se adaptarem a essa realidade largarão na frente e estarão inovando em valor. Daí a importância da criação de cenários prospectivos para o desenho dos possíveis ambientes futuros, possibilitando a adoção de ações estratégicas.

## A importância da prospecção de cenários

A necessidade de as empresas conhecerem os riscos que envolvem seus negócios fundamenta a construção e a utilização de cenários prospectivos. Os riscos podem ser relacionados ao ambiente externo, aos processos internos ou às informações para a tomada de decisões. A análise do ambiente externo se faz importante, pois está ligada à viabilidade ou não do negócio. Já os processos internos podem ser decisivos na execução do modelo. As informações para a tomada de decisão devem ser confiáveis e relevantes, a fim de que todo o processo possa ser suportado.

O objetivo do gerenciamento de riscos é transformar a incerteza total em incerteza parcial, dentro do dinamismo exigido no processo de tomada de decisão. É uma questão de competitividade e, até mesmo, de sobrevivência. Assim, a elaboração de cenários prospectivos torna-se peça chave por permitir que os gestores tenham visão holística das variáveis externas.

Tendo em vista que no Brasil um dos fatores de risco que impacta mais profundamente nas operações de inúmeros segmentos empresariais é a segurança, a construção desses cenários se

apresenta como importante ferramenta de gestão para melhorar o planejamento estratégico e preparar as empresas para ameaças e possíveis oportunidades.

A partir desses estudos, o gestor pode controlar o alcance de seus objetivos estratégicos e alterar suas ações conforme o cenário. O gestor deve compreender os movimentos dos fatores e variáveis, traçando possíveis encaminhamentos e elaborando as estratégias que as empresas devem implementar.

## Crime organizado

O roubo de cargas é um crime eminentemente organizado, pois pressupõe a existência de receptadores, o envolvimento de funcionários das empresas de transporte, certa logística criminal e o emprego de informações. Atingir a estrutura das organizações criminosas é, portanto, requisito para que o poder público possa mitigar o problema.

Às empresas que atuam no setor, contudo, não cabe esperar por melhorias advindas da gestão pública ou da providência divina. É necessário conhecer o cenário em que atuam para poder traçar estratégias e escolher as melhores práticas para neutralizar o impacto negativo nos negócios.

A elaboração de cenários prospectivos é a única ferramenta capaz de permitir a avaliação correta e a antecipação dos fatos negativos. Apenas assim é possível definir e otimizar as ações operacionais e inovar em valor, criando estratégias que permitam explorar novos espaços no mercado.





Você sabe o  
**tamanho** de  
**seus** **riscos?**

# Cenários prospectivos na economia brasileira

*Análise comparativa da situação econômica prospectada em 2009 para os quatro anos seguintes e a situação real vivida em 2013 mostra a importância e eficiência da construção de cenários prospectivos para o êxito dos negócios e o cumprimento de metas em qualquer setor.*

As formas de se conduzir a economia hoje e a rápida evolução das tecnologias faz com que novos riscos apareçam no cenário econômico. Um dos principais fatores para o sucesso competitivo de um negócio é a diferenciação. O ator que conseguir olhar com maior nitidez para os próximos anos e decifrar tendências de indicadores macroeconômicos vai projetar um cenário prospectivo mais perto do real. Assim, seus esforços em prevenção e manutenção da saúde do negócio poderão alavancar nova tendência no mercado e aumentar os lucros.

Aqui vamos considerar um cenário prospectivo sobre a economia do Brasil traçado em 2009 para um período de quatro anos, pelo The Economist, e compara-lo com publicação de 2013 do mesmo jornal, avaliando se tal cenário se concretizou. O artigo escrito em novembro de 2009 com o título “Brazil takes off” (“O Brasil decola”) apontava que o país estava em plenas condições de crescimento sólido, listando pontos fortes e oportunidades de alavancagem de negócios, mas também as ameaças que poderiam atrapalhar aquele cenário. O artigo escrito em setembro de 2013 trouxe o título “Has Brazil blown it?” (“O Brasil estragou tudo?”), pois as boas perspectivas traçadas em 2009 não vingaram e apontou fatos negativos que barraram o crescimento prospectado.

Segundo o The Economist, O Brasil deu uma reviravolta no cenário, começou a reagir e tomar as rédeas do setor econômico-financeiro em meio à crise imobiliária nos EUA em 2008. Enquanto o fundo de investimento estrangeiro teve alta de 30% no

país, a média mundial foi de 14%. O Brasil era apontado, dentre os integrantes do BRIC – bloco formado por Brasil, Rússia, Índia e China –, o de melhor perspectiva, pois ao contrário da China é um país democrático, não possui problemas religiosos e étnicos comparáveis aos da Índia e possui maior variedade de produtos para exportação que a Rússia.

Em 2007, o Brasil descobriu grandes reservas de petróleo, enquanto a China se consolidou como potência mundial mais populosa do mundo. Com isso, aumentaram as demandas por minério e alimentos, as commodities atingiram preços altos e fortaleceram a economia e as oportunidades no Brasil, que também foi eleito sede da Copa do Mundo de 2014 e dos Jogos Olímpicos de 2016, fatores que deveriam alavancar ainda mais a economia. Economistas fizeram previsões de futuro para o Brasil e apontavam que em 2014 o país seria a 5ª maior economia do mundo e a cidade de São Paulo a 5ª mais rica do mundo, posição ocupada hoje por Genebra, capital da Suíça.

## Valor agregado pelas reservas naturais e condições climáticas

A abundância dos recursos naturais colocavam o Brasil em posição privilegiada e aumentava seu potencial de crescimento. É o país com a maior reserva de água doce do mundo, com terras inexploradas e férteis em várias regiões nas quais se consegue executar três ciclos de cultivo ao ano, condições climáticas favoráveis e grandes reservas de minério e petróleo. Em 2009, foi registrado crescimento econômico superior a 5% e a projeção do

PIB para os anos seguintes era das melhores.

A mesma matéria do The Economist ressaltava, porém, as fraquezas que assolavam o Brasil naquela época e deveriam ser combatidas, sob pena de os resultados prospectados não serem viabilizados e o país voltar à estagnação. Especialistas do jornal destacaram, além do sucesso estar fundamentado em commodities e haver necessidade de investimentos no setor produtivo, os seguintes fatores a serem tratados para a manutenção do crescimento do Brasil:

*Máquina pública extremamente onerosa e baixos investimentos nos setores público-privado;*

*Gastos do governo aumentam mais rápido que o crescimento da economia;*

*Recursos arrecadados da população mal-empregados;*

*Altas taxas e impostos sobre bens e serviço, impactando população e empresários;*

*Os sistemas de seguro social e pensões extremamente onerosos e paternalistas;*

*Infraestrutura precária;*

*Educação sucateada;*

*Alta taxa de assassinatos;*

*Corrupção envolvendo a maioria dos políticos;*

*Diferenças sociais.*

Quatro anos depois, o jornal norteamericano buscou avaliar o que deu errado em sua projeção. Apesar de em 2010 ter sido registrado aumento de 7,5% no PIB, maior alta em 25 anos, em



2011 o crescimento já caía para 2,7%. Os gastos públicos continuavam altos, o setor privado sobrecarregado com mais impostos e o país começava a apresentar baixos sinais de competitividade. Em 2012, o crescimento do PIB tem queda brutal, ficando em apenas 0,9%. Paralelamente, os EUA voltavam a se reerguer da crise e os países emergentes desaceleraram. O preço das commodities, principal fonte de riqueza do Brasil, despencou.

Em 2013, os especialistas já apontavam fatores que, entre 2009 e 2013, impediram a economia brasileira de se manter sólida e constante. As vias de escoamento da produção continuaram precárias e os gastos públicos aumentaram para 60% a 70% do PIB nacional, o que provocou desconfiança dos investidores com o governo e desacelerou os investimentos no país.

## Nada foi feito para sustentar o crescimento

Nenhum dos itens da lista de preocupações feita em 2009, que podiam ameaçar o crescimento, recebeu a devida atenção do governo. Reformas políticas não aconteceram, os investimentos em infraestrutura também não e os serviços públicos como educação, saúde e segurança continuaram ineficientes. Houve retração no setor de serviços e o consumo foi freado pela tensão na economia.

O que poderia ter sido feito para evitar esse ambiente desfavorável para o país? O trabalho de construção de um cenário futuro foi correto. Os riscos e os atores responsáveis foram iden-

tificados e com eles as áreas nas quais se deveria agir. De 2009 a 2011, o crescimento do PIB ficou entre extraordinário e bom. A falta de ações adequadas, corretivas ou de manutenção do cenário, foi responsável pela queda tão brutal a partir daí.

## Cenários precisam ser reavaliados com disciplina

A formação de cenários prospectivos é extremamente útil para tomada de decisões. Mas as revisões dos cenários e as respectivas análises de risco devem ser executadas com disciplina e precisão. A atualização do cenário e o constante monitoramento sobre o surgimento de novos riscos ou a modificação dos riscos já existentes é fundamental.

O artigo de 2009 publicado pelo jornal projetava um cenário prospero para o Brasil, mas dependia de ações e iniciativas previstas para a sustentação do crescimento econômico do país. Vimos em 2013 que o acompanhamento e monitoramento dos atores do cenário e o tempo de reação não foi considerado. Alguns fatores importantes não receberam a devida atenção.

O cenário prospectivo traçado em 2009 correspondeu aos riscos concretizados em 2013, mas para mostrar inatividade dos responsáveis. Este estudo reforça a ideia de que a gestão de riscos bem feita, incluindo a projeção de cenários, a avaliação periódica dos riscos e a consequente remodelagem dos cenários é ferramenta essencial para a mitigação dos riscos e alcance dos resultados projetados.

# A segurança corporativa como parte da estratégia dos negócios

*A elaboração de cenários prospectivos nos leva a análises de condições futuras, mostrando possíveis caminhos a serem percorridos e decisões assertivas a serem tomadas considerando as incertezas e ameaças dos riscos que estão a todo tempo nos desafiando; o modelo agrega valor no escopo proposto pelo planejamento estratégico das empresas, com metodologias plausíveis e atuações mais focadas.*

Segurança é um assunto comentado em todos os cantos do mundo e discutido em todos os modelos de negócios, seja no setor público ou privado. Hoje, observo nos diversos setores departamentos de segurança atuando apenas operacionalmente, o que dificulta inclusive aos executivos enxergarem os valores que o departamento pode agregar dentro do estratégico.

E como fazer o direcionamento estratégico para área? Os processos e procedimentos de segurança corporativa devem ser pensados sempre como atuações preventivas e antevendo as ameaças internas ou externas. Para o sucesso da gestão estratégica, dos ambientes internos, externos e o seu devido monitoramento, as diversas ferramentas de cenários prospectivos permitem definir a estratégia com flexibilidade e aderência ao negócio.

Os cenários não são a estratégia propriamente desenvolvida, mas dependem de atitude e interpretação daqueles que os elaboram e de seus executores. Entre as vantagens da elaboração de cenários, estão:

*Entender o ambiente*

*Lidar com a incerteza*

*Visão do negócio*

*Ajudar na criatividade*

*Identificar oportunidades*

A segurança corporativa nas organizações não deve ficar só no nível tático operacional, com monitoramento dos vigilantes em postos, rondas, CFTV's etc. O departamento tem capacidade maior para enxergar e atuar nos riscos corporativos, trazendo

resultados potenciais para o negócio com influência no lucro líquido, mitigando e eliminando riscos, o que pode colocar a empresa em posição de destaque.

Se o departamento não tem a mesma importância como as áreas de marketing ou comercial, os problemas relacionados à segurança podem ter soluções parciais ou incompletas, provavelmente por sua atuação tática operacional e pouco estratégica. Por isso é preciso projetar o futuro com método e foco para o seu bom desempenho.

Os departamentos de segurança corporativa devem sair do convencional e uma das chaves é inovar valores. Nas empresas, a segurança tem dificuldade de colocar em prática não apenas o pensamento, mas também a escrita. A matriz de avaliação de valor pode ser um instrumento analítico para inovação de valores e diagnóstico do modelo de desenvolvimento estratégico ideal.

*O que eliminar?*

*O que iremos focar?*

*O que precisaremos aumentar?*

*O que é preciso criar para pensar no novo?*

A prospectiva não pode estar separada da estratégia e não pode chegar à visão de apenas uma antecipação, deve ser norma de abordagem e reflexão. O pensamento de longo prazo só existirá se forem integradas prospectivas e estratégia e se, culturalmente, houver o entendimento dos autores da empresa.

Precisaremos conhecer bem os ambientes estratégicos para construir os cenários prospectivos do departamento e não ficar

apenas no nível operacional. Deve-se pensar a estrutura de segurança corporativa focada no pleno entendimento das questões estratégicas para pensar o futuro de forma planejada, com métodos eficazes e foco nos objetivos, respondendo às perguntas:

*O que fazer para enfrentar?*

*O que fazer para mitigar?*

*O que monitorar?*

Ao obter as respostas, o departamento vai trabalhar naquilo que gera valor, centrado em planos de longo prazo e com monitoramento constante, atuando de forma preventiva e mitigando riscos de forma a potencializar os negócios da organização.

À medida em que vou evoluindo no curso MBA em Gestão de Riscos Corporativos, fica mais clara minha visão sobre o momento dos diferentes negócios no setor corporativo da segurança. Os gestores não lançam novos modelos de planejamento que poderiam permitir ao negócio se diferenciar no mercado.

Boa dica é o gestor de segurança compreender bem as ferramentas e metodologias de avaliação de cenários, mantendo a área alinhada ao escopo do planejamento estratégico e toda sua estrutura. Nesse contexto, para definição de suas ações o gestor deve desenvolver cenários prospectivos e a utilização de metodologia correta traz assertividade ao planejamento.

Ao conduzir a atuação do departamento conforme a direção estratégica do negócio, os executivos com certeza terão visão do valor agregado pela área, que deixará de ser vista como centro de despesa dentro da organização.



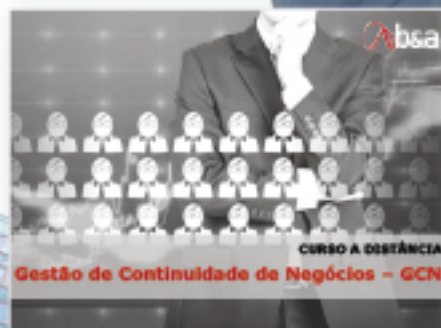
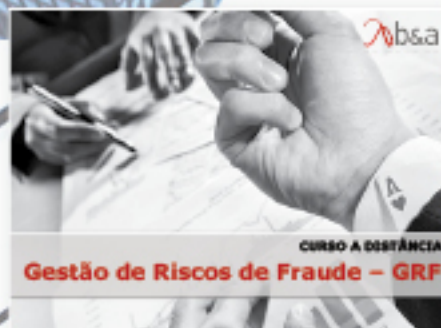
# ENSINO A DISTÂNCIA DE ALTA EXCELÊNCIA GESTÃO DE RISCOS CORPORATIVOS

DE ONDE  
VOCÊ ESTIVER  
NA HORA  
QUE QUISER



Vídeos on line, por  
módulo, com o  
**Prof. Dr. Antonio  
Celso Ribeiro  
Brasileiro**

Exercícios práticos,  
apostilas, livros e  
certificado



**ab&a**  
BRASILEIRO ASSOCIADOS

**Sicurezza**  
EDITORA

[www.sicurezzaeditora.com.br](http://www.sicurezzaeditora.com.br) - (11) 55316171

## **Auditoria de Plano de Continuidade de Negócios**

16 horas – Profa. Andrea Thomé - 18 e 19 de agosto, das 8h30 às 17h30

## **Planejamento em Segurança Eletrônica**

40 horas – Prof. Marcelo Barbosa - 17 a 21 de agosto, das 8h30 às 17h30

## **Implantação de Modelo das 3 Linhas de Defesa para Cobertura de Riscos Tecnológicos e de Segurança da Informação**

16 horas – Profa. Andrea Thomé - 27 e 28 de agosto, das 8h30 às 17h30

## **MBS (Master Business Security) - Avançado em Segurança Empresarial - 48ª Turma**

120 horas - Coordenação prof. dr. Antonio Celso Ribeiro Brasileiro - início 12 de setembro (aulas aos sábados), das 8h30 às 17h30

## **Prevenção e Combate à Incêndios**

16 horas – Prof. Celeste Aparecida da Silva - 19 e 26 de setembro, das 8h30 às 17h30

## **Plano de Continuidade de Negócio, incluindo Resposta e Gestão de Emergência e Crise**

24 horas - Profª Sandra Alves - 21 a 23 de setembro, das 8h30 às 17h30

## **Auditoria do Modelo de Governança Corporativa com Base no Framework do IBGC**

16 horas – Prof. Andrea Thomé - 24 de setembro, das 8h30 às 17h30





## GESTÃO DE CONTINUIDADE DE NEGÓCIOS GCN

*Antonio Celso Ribeiro Brasileiro*

A nova obra de Antonio Celso Ribeiro Brasileiro, publicada pela Sicurezza Editora, é de extrema importância para as empresas de grande, médio e pequeno porte, pois os riscos acontecem independentemente do tamanho do negócio. Os riscos podem ocorrer em qualquer situação, sejam provenientes de catástrofe natural, gerados por falha humana ou técnica, de crédito, imagem, estratégico, operacional, de impacto ao meio ambiente, entre outros.

O livro detalha um processo de continuidade de negócio com sustentação de um plano de medidas preventivas e melhorias contínuas para as empresas, buscando o fortalecimento do negócio. O livro do professor Brasileiro, assim conhecido no mercado de consultoria em gestão de riscos corporativos, apoia alunos, gestores, administradores, facilities, engenheiros e outros interessados na construção de um plano de continuidade de negócios, incluindo medidas contingenciais e de emergência.

cios, incluindo medidas contingenciais e de emergência.

“A intenção de aceitar o risco não equivale ao desejo irresponsável de apostar na sorte” é a frase, de um autor desconhecido, que norteia o comentário final do livro para análise e reflexão de todos os leitores.

**2014 - 240 págs. - R\$ 45,00**



INVESTIGAÇÃO CRIMINAL -  
UM ESTUDO METODOLÓGICO

Luis Henrique Costa Ferreira e  
Nilton José Costa Ferreira

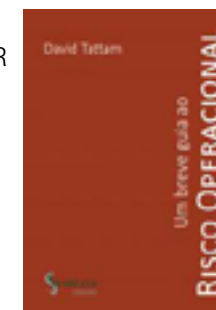
2013 - 427 págs. - R\$ 35,00



RISCOS DE FRAUDE  
UM BREVE MANUAL PARA PREVENIR  
E DETECTAR FRAUDES

Nigel Iyer e Martin Smociuk

2013 - 197 págs. - R\$ 28,00



UM BREVE GUIA AO  
RISCO OPERACIONAL

David Tattam

2012 - 232 págs. - R\$ 28,00



Críticas e sugestões de pauta:  
[revista@brasiliano.com.br](mailto:revista@brasiliano.com.br)

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

Edição 87 - Julho 2015

ISSN 1678-2496N

A revista Gestão de Riscos é uma **publicação gratuita** eletrônica da Brasiliano & Associados  
Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL

Direção: Antonio Celso Ribeiro Brasiliano e Enza Cirelli

Edição: Robson Regato

Edição de arte: Marina Brasiliano