REVISTA
GESTÃO DE RISCOS

b&a BRASILIANO & ASSOCIADOS

EDIÇÃO 103
NOVEMBRO 2016

02 ponto de vista
2016 um ano de susto: faltou inteligência em riscos?

5 Inteligência empresarial: foco em processo de antecipação e emprego nas empresas

14 Inteligência em riscos corporativos: o verdadeiro valor agregado nos negócios das organizações. Você possui?

21 Inteligência empresarial

25 O Brasil é vulnerável aos Cyber Riscos. Os gestores de riscos estão preparados?

31 Ler e saber: Novo livro digital GRATUITO

2016 um ano de susto: faltou inteligência em riscos?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS

Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano & Associados Gestão de Riscos.

abrasiliano@brasiliano.com.br

ponto de vista

Planejamento orientado por cenários e gestão em riscos corporativos tornam-se uma exigência cada vez maior, em um mundo mais VICA: Volátil, Incerto, Complexo e Ambíguo! Como essa prática pode nos ajudar a acertar? Em 2016 foi complicado!

Mal tinha começado e já estava sendo chamado de pior ano da história. Era uma hipérbole, mas terrorismo, zika, David Bowie morto... estava com jeitão de que não iria bem. E foi ficando surpreendente cada vez mais! 2016 foi o ano do NÃO ÓBVIO. O povo inglês disse sim para sair da União Europeia, Trump Presidente dos Estados Unidos da América. Portanto um ano atípico e muito emocionante, que serviu para lembrar a todos nós que o imprevisível acontece, o famoso CISNE NEGRO.

As decisões são tomadas no presente para surtirem efeitos no futuro. No entanto, o futuro é desconhecido e incerto. As condições podem ser completamente outras que planejamos. As incertezas associadas e interconectadas geram uma grande necessidade de adaptação que exige do gestor uma capacidade de realizar uma abordagem multidimensional como ambidestria. Ter a capacidade de alternar estratégias de acordo com a volatidade e agressividade do ambiente, seja ele qual for!

Por exemplo, o trágico acidente da Chapecoense na madrugada de 29 de novembro, deixou muita tristeza e muitas lições. E 71 mortos é um preço altíssimo e absurdo a pagar neste e em qualquer aprendizado. Nada disso era necessário para saber que não se decola com um plano de voo extremamente justo, um plano de voo de risco, complicado na fase final por um evento inesperado: a ocorrência de uma emergência declarada por outro avião na mesma área, um A-320 com vazamento de combustível. Com isto o Avro RJ85 da LaMia, foi obrigado a dar mais voltas do que esperava e com isto, a pane seca acabou concretizando e o avião colidiu a 30 km do aeroporto de Medellín. O comandante boliviano Miguel Quiroga, era experiente, jogou com a sorte? Acreditou que pudesse vencer a distância justa de 2.985 km, apenas 15 km abaixo do alcance máximo do jato, cerca de 3 mil km, sem ter que abastecer? Faltou uma boa análise de riscos e cenários? Foi negligente? Imprudente? O órgão regulador boliviano que aprovou o plano de voo foi conivente? O acidente da LaMIa foi a amarga cereja deste bolo de difícil digestão que é o ano de 2016.

Ano pródigo em emoções cujos trancos foram abundantes no Brasil. Toda uma linha sucessória foi dizimada. Uma presidenta da República, um presidente da Câmara dos Deputados e um do

ponto de vista

Senado! Este, depois de afastado, foi reintegrado ao cargo, mas afastado da linha sucessória. Tudo isso em menos de cem dias. O vice-presidente Michel Temer assume, cheio de convicções reformistas e, meses depois, já vivia uma crise. Seis ministros deixaram o governo, assombrados por delações. O desequilíbrio dos três poderes faz com que a nossa "escala Richter" beire dois dígitos e o tsunami é surfado pela Justiça Brasileira, em função da mediocridade dos poderes Legislativo e Executivo.

Com isso tudo, o que podemos esperar de 2017? Vamos continuar em forte turbulência? Os especialistas de diversas áreas dizem que sim!

Daí mais do que nunca, cresce a importância dos gestores aplicarem corretamente os conceitos da Inteligência em Riscos Corporativos, tendo como premissa a interconectividade entre as inúmeras disciplinas de riscos e a construção de cenários prospectivos. Organizar de forma lógica e tangível todas as variáveis envolvidas é o desafio enfrentado, além da flexibilidade necessária para lidar com todas as partes interessadas no negócio da organização.

Estimular continuamente nossa forma de pensar e a capacidade de autorreflexão é um aspecto fundamental para desenvolver e manter a vantagem ofensiva. Precisamos possuir uma grande acuidade perceptiva, enxergar neste mar de incerteza as oportunidades, divisar um novo caminho, se comprometer com ele e principalmente fazer com que a nossa organização seja flexível e ágil.

Conseguiremos?

Boa leitura e sorte!

Mariana A. de Melo
Especialista em Gestão de Riscos pela FAPI/Brasiliano & Associados e Gestora de Riscos.

Inteligência empresarial: foco em processo de antecipação e emprego nas empresas

A inteligência empresarial com foco em processo de antecipação e emprego nas empresas engloba riscos dentre a contratação e o exercer da função no dia-a-dia.

A inteligência empresarial na organização, consiste no processo de obtenção, análise de dados, produção e disseminação de informações úteis aos indivíduos e nas organizações, de acordo com suas necessidades.

Pode se dizer que inclui, também, a proteção do conhecimento disponível na organização.

Neste cenário, a inteligência empresarial é o suporte ideal para a produção e salvaguarda dos dados e informações de interesse das altas administrações.

Quando Drucker começou a estudar gestão de empresas, logo após a II Grande Guerra, um administrador era definido como “alguém que é responsável pelo trabalho e por seus subordinados”, o patrão ou o chefe. Drucker sugere que esta definição mude para alguém que “é responsável pela aplicação e desempenho do conhecimento”. Isto significa que a gestão passa, hoje, por usar o conhecimento existente na organização para gerar melhores resultados. Os grandes ganhos de produtividade, daqui para frente, advirão das melhorias na gestão do conhecimento.

A produtividade do conhecimento deve ser, portanto, a preocupação central dos administradores do século XXI. No entanto, o conhecimento só será produtivo se gerenciarmos toda sua cadeia de valor/valores. As empresas querem ser produtivas para serem mais lucrativas. E a lucratividade e competitividade são as verdadeiras determinantes da inovação tecnológica e do crescimento da produtividade. Assim, não podemos nos contentar em gerar novos conhecimentos, em fazer apenas a pesquisa pela pesquisa, ou simplesmente em coletar informações e guardá-las. Sem capacidade de inovar, criar novos produtos e serviços, mas também, de criar novos mercados, exportar e empreender negócios, nenhuma empresa se tornará líder em seu setor ou mesmo conseguirá sobreviver nesta economia globalizada.

Pode se definir que Inteligência Empresarial (ou Inteligência de Negócios) é a capacidade de uma empresa propõe em capturar, selecionar, analisar e gerenciar as informações relevantes para a gestão do negócio com o objetivo de (Teixeira 2009):

- Inovar e criar conhecimento;
- Reduzir riscos na tomada de decisão e evitar surpresas.
- Direcionar, assertivamente, os planos de negócios e a implementação de ações;
- Criar oportunidades de negócios;

As empresas querem ser produtivas para serem mais lucrativas. E a lucratividade e competitividade são as verdadeiras determinantes da inovação tecnológica e do crescimento da produtividade.

- Apoiar o desenvolvimento de produtos/serviços com uma base de informação confiável, eficiente e ágil;
- Monitorar, analisar e prever, eficientemente, as questões relacionadas ao core business;
- Gerar valor aos negócios.

A Inteligência Empresarial pode ser concebida como o resultado de uma evolução como função híbrida do planejamento estratégico e das atividades de pesquisa de marketing. (Tyson 1988).

A Inteligência Empresarial busca integrar os sistemas computacionais aos sistemas de informação organizacionais, enquanto o BI (Business Intelligence) concentra-se no desenvolvimento de sistemas de informação computacionais. (Matheus; Parreiras, 2004).

A Inteligência Empresarial pode ser concebida como o resultado de uma evolução como função híbrida do planejamento estratégico e das atividades de pesquisa de marketing. (Tyson 1988).

Portanto, a Inteligência Empresarial não se limita à tecnologia, assumindo posição de destaque na tomada de decisão estratégica de diversas categorias de usuários como executivos, gerentes e analistas.

Se levarmos em consideração que o objetivo da inteligência é transformar informação subjetiva e desagregada em vantagem competitiva para agregar valor aos negócios, é natural que qualquer área possa construir a sua base de inteligência. Assim podemos ter, não só a inteligência de mercado ou competitiva, constantemente pela mídia, como também inteligência de produtos, inteligência de logística, inteligência de clientes, inteligência financeira e assim por diante. (Teixeira 2007). Essas inteligências, juntas, constituem a inteligência empresarial.

Neste contexto, a Inteligência de Mercado ou Competitiva (IC) é parte da Inteligência Empresarial e engloba, principalmente, informações sobre o mercado e a concorrência. (Teixeira 2009)

Segundo a SCIP - Society of Competitive Intelligence Professionals (www.scip.org), a inteligência competitiva é um programa sistemático e ético para coleta, análise e gerenciamento de informações externas que podem afetar os planos, decisões e operações de uma empresa.

Como a teoria é, muitas vezes, diferente da prática no ambiente empresarial, a área de inteligência competitiva acaba abrangendo muito mais do que informações externas (mercado e concorrência), sendo responsável por demandas que incluem desde dados quantitativos e performance de produtos ao mapeamento inteligente de clientes.

Insegurança

O perigo de incerteza e insegurança permeia o ambiente profissional, quando o assunto é proteção de vantagens competitivas de uma organização. Talvez essa percepção seja a consequência de uma realidade que motiva a competição extrema, na qual se encontram as organizações privadas. Vantagens competitivas organizacionais podem, em sua maioria, traduzir-se pelo simples fato de organizações possuírem algum tipo de informação ou ativo que possa ser considerado um diferencial em seu modelo de gestão. No que concerne especificamente ao âmbito organizacional, não basta somente investir em ações e técnicas relacionadas ao estabelecimento de tais vantagens competitivas. Conforme afirma a Associação Brasileira de Inteligência Competitiva (ABRAIC), torna-se fundamental, também, a aplicação de técnicas e ferramentas para a manutenção dessas vantagens, incluindo a proteção do chamado conhecimento sensível, ou vantagens competitivas para os fins deste artigo. Percebe-se que as necessidades de segurança em um ambiente organizacional tornam-se válidas somente após a ocorrência de determinado incidente.

As possíveis perdas organizacionais são diversas, desde o vazamento de informações sigilosas ao colapso de infraestruturas que sustentam a viabilidade de determinados negócios. Dos vários entendimentos sobre como manter protegidas tais informações, um se sobressai, o de que evitemos ao máximo precisar utilizar contramedidas para a proteção de conhecimento sensível no ambiente organizacional. Isso devido à sua complexidade e à possibilidade de obtermos resultados imprevistos.

Todavia, no instante em que tais ações são necessárias, elas devem estar implementadas e aptas para a proteção e defesa da organização. Tendo em vista esse cenário, as seguintes questões tornam-se pertinentes à pesquisa:

- Como identificar de maneira sistemática o escopo de diferenciais competitivos em ambientes organizacionais?
- O que precisa mudar nas organizações com vistas à manutenção de tais vantagens competitivas?
- Existem mecanismos de proteção que podem ser implementados em ambientes organizacionais com vistas a amenizar essa insegurança?

Sendo assim, o objetivo é propor um método para identificar mecanismos de proteção no ambiente organizacional em convergência com conceitos relacionados à Contra inteligência (CI) e utilizar uma sistemática de Gestão de Riscos (GR) para a identificação e avaliação de riscos, como proposição para delimitar o que precisa ser protegido no ambiente organizacional.

Emprega dois ramos distintos que interagem e se complementam:

Inteligência e Contra Inteligência. A inteligência produz os segredos da empresa e a Contra Inteligência previne e neutraliza ações de pessoas, organizações ou inteligência adversa.

Contra inteligência

A contra inteligência pode ser entendida como sendo o conjunto de ações que objetivam identificar e neutralizar as ações de espionagem. Pela perspectiva civil, conforme a ABRAIC (2008), tais ações buscam invasor, neutralizar sua atuação, recuperar, ou mesmo contra-atacar por meio da produção de desinformação. As definições de contra inteligência são oriundas do contexto militar e de segurança de estado. Os métodos de contra inteligência foram desenvolvidos e adaptados a partir de técnicas aplicadas de proteção.

Inteligência empresarial e gestão de risco

Neste assunto, surge a possibilidade de haver risco que conduz a inteligência empresarial, é necessário haver uma gestão que possa identificar ameaças e vulnerabilidades que colocam o negócio em perigo, elaborando análises, emitindo alertas, que permitam decisões seguras e viáveis. O risco acompanha o homem e é inerente a sua natureza, também pode ser compreendido a um efeito da incerteza que fatores internos e externos, trazem sobre sua concretização de objetivos determinados, o risco existe, além de ser acompanhado de aprendizado e escolha de caminhos de desenvolvimento.

Investigação de funcionário para contratação

Hoje, para a contratação de qualquer colaborador, exige-se a submissão a extensa bateria de exames, testes vocacionais, dinâmica de grupo, entre outros. A contratação de empregados, notadamente os que serão aproveitados em áreas de maior relevância dentro da instituição, precede a uma acurada verificação de histórico, que acontece desde a entrevista inicial até a efetiva contratação.

As checagens mais comuns visam a verificar a capacidade de exercer liderança, distribuir tarefas, atribuir responsabilidades, suportar pressões e tomada de decisões. Esses requisitos são avaliados principalmente quando a empresa pretende que o candidato a emprego cresça profissionalmente na corporação, criando um vínculo extenso de compromisso moral e social.

Entretanto, tem se tornado cada vez mais comum por parte das empresas realizar uma análise comportamental dos candidatos a vagas de emprego. Isso acontece até mesmo porque cada vez mais tanto as empresas públicas como as privadas vêm sendo solicitadas a prestar contas por ações de seus funcionários como indivíduos. Sendo assim, o ideal seria encontrar profissionais que se adequem da melhor forma possível ao modelo e à visão propostos por ela.

Outra tendência, e desta vez polêmica, verificada no mercado de trabalho é a exigência da apresentação de alguns atestados de antecedentes, quer sejam expedidos por órgãos policiais ou judiciais, além da famosa consulta a órgãos de proteção ao crédito.

Assim, a exigência de atestados de antecedentes expedidos pelos órgãos policiais ou as certidões expedidas pelos órgãos judiciais pode ser exigida para qualquer candidato a emprego. Há profissões, como no caso de vigilante, que a apresentação de atestado de antecedentes é, inclusive, obrigatória.

Conquanto uma pessoa que deva algo, para alguma instituição qualquer, pública ou privada, física ou jurídica, não mereça ser qualificado, desmerecedor de confiança no sentido literal do termo, tal situação pesa contra si, pois quem não cumpre seus compromissos, notadamente os financeiros, aparentemente poderá repetir tal desiderato outras vezes. E aqui se está a dizer do devedor contumaz, que dirige sua vida financeira sem muito critério.

O empregador deste profissional com restrições pode não dissociar sua vida particular da profissional, uma vez que ele carregará para dentro da empresa toda essa particularidade. Nesse sentido, podemos usar como exemplo o empregado bancário que emita cheques sem a suficiente provisão de fundos. Ele seria lícito de demissão, o que revela a necessidade de o empregado manter sua conduta ilibada.

Entendemos que é lícita a exigência de atestados de idoneidade, inclusive de ausência de restrições financeiras. Não se vê, nesse dever de cuidado, qualquer violação aos direitos do cidadão, até porque quem deixa de honrar um compromisso financeiro está a locupletar-se ilicitamente em detrimento do credor, situação vedada em nosso ordenamento jurídico, uma vez que a ninguém é licito de enriquecer-se ilicitamente.

Caberá ao empregador, diante de um fato em concreto, donde se pleiteie reparação por danos provocados por um empregado, mesmo se cobrado por outros funcionários, demonstrar que agiu diligentemente para evitar uma contratação indevida.

Nessa linha de raciocínio, o direito de ingresso em juízo é público e subjetivo, portanto se um candidato se julgar prejudicado por algum fato de seu passado ou consulta que não digam respeito à sua vida profissional, poderá acionar a empresa em juízo, para se ver ressarcido de algum dano que entenda ter sofrido; mas não para se ver contratado pela empresa, pois a recusa na admissão é direito protestativa do empregador.

Para concluir, numa análise macro das “Inteligências”, se levarmos em consideração que o objetivo da Inteligência é transformar informação subjetiva e desagregada em vantagem competitiva para agregar valor aos negócios, é natural que qualquer área possa construir a sua base de Inteligência. (Teixeira 2007).

A conclusão deste trabalho considerou como base o modelo de proteção de inteligência empresarial, que possui como premissa considerar o valor do tempo da informação. Corresponde a um entendimento de como uma organização se mobiliza para identificar e quantificar o potencial da perda, se tiver qualquer tipo de ataque de inteligência no seu ambiente. Entende-se que isto é fundamental para se amenizarem os eventuais resultados negativos. Dos vários entendimentos sobre como manter protegidas tais vantagens competitivas, uma se sobressai, a de que se evite ao máximo precisar aplicar contramedidas para a proteção organizacional. Visto que a importância para uma boa contratação de um colaborador, é verificar a procedência do indivíduo, tal como sua origem, experiência e valores.

as metodologias e disciplinas de risco da sua empresa estão integradas?

a sua empresa utiliza alguma tecnologia para facilitar o controle dos riscos?

INTELIGÊNCIA em RISCOS é a SOLUÇÃO

b&a

BRASILIANO&ASSOCIADOS

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS
Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano & Associados Gestão de Riscos.
abrasiliano@brasiliano.com.br

Inteligência em riscos corporativos: o verdadeiro valor agregado nos negócios das organizações. Você possui?

O atual contexto de Gestão de Riscos Corporativos das organizações, no Brasil e no mundo, está cada vez mais complexo e dinâmico, exigindo um processo com alta flexibilidade e mantendo um nível elevado da área de gestão de riscos, bem como uma maior tempestividade na avaliação contínua e na resposta a potenciais cenários de riscos.

A dinamicidade do mercado e as inúmeras disciplinas de riscos corporativos que hoje o gestor é obrigado a lidar e gerenciar, faz com que estas variadas disciplinas estejam debaixo do mesmo Framework, falando a mesma linguagem, de tal forma que possa haver uma interpretação das informações relevantes gerando a verdadeira inteligência em riscos na organização. Esta Inteligência em Riscos Corporativos, integração das disciplinas, agrega valor e previne contra as incertezas do ambiente de negócios, ajudando a empresa a priorizar recursos. No entanto, outro desafio prioritário é integrar a estrutura de gestão de riscos aos processos e às estratégias da organização. Além de mensurar os riscos da empresa, o objetivo destacado pelas organizações é a criação de uma função integrada às estratégias da organização, que gere e preserve valor aos acionistas.

Hoje podemos dizer que o mercado empresarial passa pelo que chamamos de VUCA, uma sigla utilizada para descrever a volatilidade (volatility), a incerteza (uncertainty), a complexidade (complexity) e a ambiguidade (ambiguity) nos ambientes e situações de negócio. VUCA em inglês, VICA em português. Oriunda do vocabulário militar americano, o uso comum do termo VUCA começou no final dos anos 1990. O conceito VUCA expressa a complexidade da nossa sociedade contemporânea, devido à interdependência e a globalização, situações que antes tinham pouco impacto, mas que agora refletem em toda sociedade. Por exemplo, a catástrofe de Fukushima, em 2011, fez as montadoras japonesas no Brasil pararem suas linhas produtivas devido à falta de peças. Ou seja, a interdependência é uma realidade no mundo globalizado e deve fazer parte da gestão de riscos.

Partindo desta abordagem, o US Army War College formulou um programa de formação para o desenvolvimento das lideranças militares, ao nível estratégico, o qual contempla a adoção de metodologias adequadas para enfrentar o VUCA e fazer frente a um ambiente extremamente agressivo e predatório. O US Army College, caracteriza os componentes deste contexto envolvente do seguinte modo:

- ***Volatilidade:*** *é marcada pelo ritmo elevado com que ocorrem mudanças com impacto na vida das sociedades desenvolvidas e concomitantemente, nas suas organizações. Assim, no atual contexto de uma Era da Informação e do Conhecimento, os dados e as evidências existentes no momento presente podem não ser suficientes para a tomada de decisão. Antecipar e prever o que pode acontecer, por exemplo durante o período de execução de um projeto, são dimensões, por vezes absolutamente decisivas.*
- ***Incerteza:*** *é uma característica do contexto marcada pela necessidade de se assumir que o conhecimento sobre uma dada situação é sempre incompleto, potencializando deste modo o aparecimento de opiniões divergentes sobre a melhor estratégia a prosseguir, exigindo uma cuidadosa análise do risco. De fato, é cada vez mais difícil levantar cenários futuros com base em acontecimentos passados.*
- ***Complexidade:*** *característica do contexto envolvente que está associada à dificuldade de compreender o*

resultado das interações dos vários componentes de um sistema, uma vez que estes raramente são de natureza mecanicista e linear. A Teoria da Complexidade vem, deste modo, mostrar a interdependência essencial de todos os fenômenos. Neste ponto, a assunção de fenômenos complexos, no seio de uma organização, impõe a necessidade de admitir interações não-lineares entre os componentes do sistema, com consequências que se multiplicam rápida e imprevisivelmente. Característica mais marcante do século XX e XXI!

- ***Ambiguidade:*** *descreve um tipo específico de incerteza que resulta de diferenças na interpretação quando as evidências existentes são insuficientes para esclarecer o significado de um determinado fenômeno. Na prática, no âmbito da gestão das organizações, a consequência deste fato é a elevada probabilidade das lideranças poderem interpretar, legitimamente, eventos de formas diferentes, aumentando significativamente a probabilidade de erros na interpretação dos mesmos. A imprecisão da realidade, o potencial de erros de leitura, os significados mistos de condições; a falta de ação, confusão entre causa e efeito e a falta de clareza. Para Greg Hutchins, especialista americano em gestão da qualidade e gestão de risco: "nós estamos saindo de um mundo linear de saber a solução dos problemas e tomar uma decisão clara para um mundo dinâmico de entender o sentido, de tomada de decisão baseada no risco, em condições VUCA."*

O mundo VUCA e/ou VICA só pode ser gerenciado com base em riscos. Daí a importância de todos os gestores saberem e/ou possuírem a competência de lidar com as incertezas.

O mundo VUCA é baseado na própria gestão de riscos, lidando com cenários complexos e altamente dinâmico, onde se exige dos gestores:

- Visão do todo e não da parte, o gestor tem que enxergar a floresta e não a árvore;
- Grande velocidade na tomada de decisão (o movimento é mais importante, não podemos ficar parados, se ficarmos o inimigo mata! O ótimo é inimigo do bom, conhecem?);
- Não ortodoxa, pensar fora da caixa, não dogmatizar soluções, ser criativo diante das incertezas;
- Colaboração e co-criação entre as equipes, redes de colaboração, estar conectado para o entendimento rápido do contexto;
- Agilidade, saber mover-se com grande flexibilidade, possuir estrutura leve para poder carregar.

O mundo VUCA é um mundo que para ser vencido é preciso possuir estes preceitos, o velho novo conceito da Gestão de Riscos. Por esta razão que a Gestão de Riscos deve ser internalizada nas empresas de forma a possuir capilaridade em todos os processos e respectivos níveis organizacionais. Com isto, a média e alta gerência das organizações estarão aptas a lidarem com o mundo VUCA e desta forma, a empresa terá uma grande vantagem competitiva frente aos seus adversários.

Após um grande período de economia pujante, o temor de uma recessão voltou a assombrar nós brasileiros. As incertezas econômicas e políticas impulsionam esse cenário desafiador no Brasil, e ainda não há uma perspectiva clara de quanto tempo ele durará e qual é sua real profundidade.

Após um grande período de economia pujante, o temor de uma recessão voltou a assombrar nós brasileiros. As incertezas econômicas e políticas impulsionam esse cenário desafiador no Brasil, e ainda não há uma perspectiva clara de quanto tempo ele durará e qual é sua real profundidade.

Além do esgotamento de um modelo de crescimento com base no consumo, o País convive com inseguranças que afetam o mercado de forma mais ampla, como custo de energia, escassez de recursos hídricos, falta de profissionais qualificados e mudança demográfica dos consumidores. Some-se a isto volatilidade do câmbio, aumento da taxa de juros e pressão inflacionária, e aí temos um "VUCA" perfeito para gerenciar.

Crises são cíclicas, inevitáveis e sempre desafiadoras, mas sempre é possível aos líderes aproveitar as oportunidades vindas com elas para obterem uma vantagem competitiva e melhor posicionarem suas empresas para o momento de retomada do crescimento.

Hoje em dia a visão e o escopo do gerenciamento de risco corporativo, dentro deste contexto turbulento ficou muito mais amplo, muito mais holístico, abrangendo inúmeras disciplinas de riscos, decorrentes das atividades desenvolvidas nas organizações. A alta direção deve ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e ou estratégicas. Para este fim, é necessária a criação de uma área específica, com uma estrutura e recursos definidos.

Por esta razão, é que este departamento deve possuir processo sistêmico e contínuo de identificação de exposição, medição, análise, controle, prevenção, redução, avaliação e financiamento de riscos. Esta nova função ajuda a integrar riscos financeiros e não financeiros tradicionais a seguros e responsabilidade legal. É uma área que possui uma grande abrangência, mas com muitas interações através de diferentes disciplinas e, portanto, com uma necessidade de uma abordagem integrada. Algumas das disciplinas de riscos que devem se interagir são:

1) Riscos estratégicos
2 Riscos operacionais – ligados a operação
3) Riscos nos processos
4) Riscos de tecnologia da informação
5) Riscos de meio ambiente
6) Riscos de saúde e segurança do trabalhador
7) Riscos de segurança empresarial
8) Riscos financeiros
9) Riscos legais

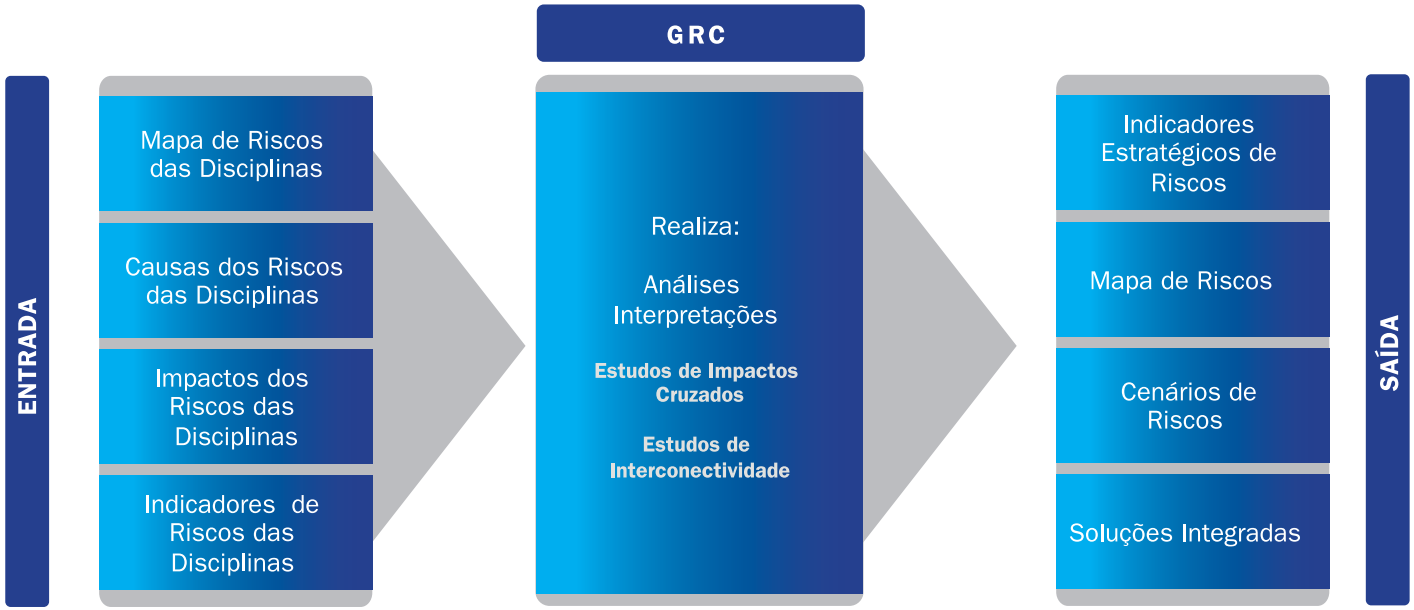
10) Riscos sociais
11) Riscos de sustentabilidade
12) Riscos de comunicação
13) Riscos de fraudes
14) Riscos na cadeia logística
15) Riscos no projeto

Estas disciplinas e outras tantas disciplinas devem estar em um único Framework e com Políticas integradas, para a empresa falar uma mesma linguagem. Este é o principal desafio das empresas, integrar as disciplinas para que possam possuir a chamada Inteligência em Riscos Corporativos – IRC.

O gerenciamento de riscos, sob este enfoque, contribui para o fortalecimento e a eficácia operacional e financeira da empresa, na medida que proporciona mecanismos de alocação de recursos para o seu emprego mais eficiente e eficaz, atingindo de forma direta a efetividade.

Portanto a função do gestor de riscos é de integrar disciplinas e gerenciar as informações das inúmeras disciplinas de riscos. O gestor de riscos tem que relacionar os diversos riscos e verificar as interdependências entre eles. Hoje por si só não existe mais a possibilidade de só ter como ferramenta de gestão a Matriz de Riscos, mas deve também ter a Matriz de Impactos Cruzados para ver a motricidade entre riscos. Segundo o Fórum Econômico Mundial, em seu Relatório de Riscos Globais de 2015: "A edição 2015 do relatório de Riscos Globais completa uma década destacando os riscos a longo prazo mais significantes ao redor do mundo, extraindo as perspectivas de especialistas e dos tomadores de decisões globais. Nesse tempo, a análise mudou da identificação dos riscos a pensar através das interconexões dos riscos e os potenciais efeitos-cascata que resultarão deles."

Podemos então afirmar que a função do gestor de riscos corporativos é possuir Inteligência em Riscos, levado para a alta administração os riscos considerados mais críticos, já com as conexões feitas. A figura abaixo mostra um modelo de gestão.



Com o modelo acima entendemos a Inteligência em Riscos em integrar soluções e indicadores, fornecendo para os decisores a visão holística dos riscos considerados críticos e as respectivas soluções integradas, com um farol de monitoramento de acompanhamento das evoluções. Desta forma a organização possuirá verdadeiramente condições operacionais de se antecipar de forma objetiva a possíveis riscos, trabalhando de forma preventiva e não só de forma reativa. A organização ganha velocidade e competitividade, fatores chaves de sucesso em um mundo VUCA!

A abrangência da área da Gestão de Riscos Corporativos é muito grande, deixando de ser somente uma abordagem financeira e regulamentar – trabalhista, tributária e de investimento. A tendência é que a área de gestão de riscos caminhe para fatores de interesse de seus stakeholders, com forte atenção à imagem e à reputação das organizações. Por esta razão a amplitude cresceu e acabou abrangendo a organização como um todo, envolvendo as médias gerências como responsáveis na gestão de riscos corporativos. Desta maneira a área de riscos passa atuar como uma área de Inteligência em Riscos, ou seja, de interpretação das informações com a utilização de ferramentas e metodologias estratégicas. A figura ao lado demonstra esta abrangência nas áreas e processos das organizações, incluindo os fornecedores críticos/estratégicos.

Abrangência da área de Gestão de Riscos Corporativos nas empresas.

Outro ponto a destacar na nova função do Gerenciamento de Riscos Corporativos e do seu Gestor, é o foco de atuação que primordialmente é o da prevenção, o da antecipação, mas também como resposta aos cenários de riscos, tem que ter estruturado respostas de emergências, descontinuidade de negócio e de crises. Atualmente o mercado identificou a necessidade de uma abordagem integrada a gestão de riscos, envolvendo temas como mercado, estratégia, modelo de negócio, segurança cibernética, anticorrupção e reputação corporativa. Essa abordagem demanda compreender e responder a interconectividade entre riscos de diferentes naturezas à medida que, e muito impulsionado pela tecnologia, os mais variados fatores podem gerar cenários de descontinuidade e de crises, impactando as operações e os respectivos resultados das empresas no curto, médio e longo prazo.

Frente a este novo contexto, mundo VUCA, torna-se imperioso que as empresas intensifiquem esforços no aprimoramento nas estruturas integradas – Inteligência em Riscos – onde o gestor possa enxergar e trabalhar tanto a prevenção como as contingências. Na verdade, a função do gestor de riscos é de um "chapéu de dois bicos": um lado a prevenção e do outro as respostas para as emergências, continuidade de negócio e crises empresariais. Tudo isso integrado em um único Framework.

A função da gestão de riscos, vista sob a ótica estratégica, atua no aumento da resiliência empresarial. Nesse sentido, a maturidade dessa função interfere diretamente na qualidade e

A função da gestão de riscos, vista sob a ótica estratégica, atua no aumento da resiliência empresarial.

entendimento global dos riscos, sejam eles internos e ou externos, que podem produzir relevantes cenários de descontinuidade e ou de crises.

O grande passo da gestão de riscos está relacionado com a definição e a qualificação de um panorama dos potenciais cenários de descontinuidade e de crise, que podem e ou devem ser gerados com base na avaliação geral de riscos operacionais, legais e estratégicos, levando em consideração a linguagem comum de riscos e o impacto para as operações e a reputação da empresa. Essa base de potenciais cenários de descontinuidade e ou de crises deverão orientar a estruturação dos planejamentos das respostas estruturadas e respectivas alternativas. É nesse momento que, deve se definir, com extrema clareza, o nível de complexidade e dimensão do impacto no contexto (empresa e sociedade como um todo).

A Inteligência em Riscos Corporativos, IRC, passa a ser então a grande arma do século XXI para o efetivo combate aos riscos emergentes, pois com o processo estruturado e seguindo a metodologia estruturada, a empresa possui grandes chances de pular na frente de seus concorrentes, adquirindo e mantendo sua real vantagem competitiva.

Carlos Eduardo Perrella
Especialista em Gestão de Riscos pela FAPI/Brasiliano & Associados e Consultor Pleno da Brasiliano & Associados.

Inteligência empresarial

- Inteligência Empresarial é a capacidade da empresa em selecionar, capturar, analisar e gerenciar as informações relevantes para a gestão de seu negócio.
- Inteligência Competitiva é a capacidade de reunir, analisar e administrar informações externas que podem afetar planos, decisões e operações de uma empresa.

No livro a Arte da Guerra, Sun Tzu fala que para suceder na guerra, a pessoa deve deter todo o conhecimento de suas fraquezas e virtudes, além de todo o conhecimento das fraquezas e virtudes do inimigo. A falta deste conhecimento pode resultar na derrota.

As transformações que ocorrem no mundo dos negócios e no ambiente organizacional podem estar diretamente relacionadas à qualidade, agilidade e processamento das informações geradas pelas empresas, especialmente quando co-relacionadas com a contabilidade gerencial, que dá suporte aos gestores na tomada de decisão.

O valor dos produtos depende, cada vez mais, do percentual de inovação, tecnologia e inteligência a eles incorporados e que os diferenciam dos concorrentes.

Organizações competitivas acumulam “inteligência” à medida que ganham sustentação

na sua vantagem competitiva, podendo considerar tal inteligência como o aspecto central para competir em alguns mercados.

A inteligência empresarial busca entender os fatores e processos humanos e organizacionais envolvidos na busca de informações, principalmente externos à organização, e na posterior tomada de decisões.

Os principais objetivos da inteligência empresarial:

- Inovar e criar conhecimento;
- Reduzir riscos na tomada de decisão e evitar surpresas;
- Direcionar, assertivamente, os planos de negócio e a implementação de ações;
- Criar oportunidades de negócios;
- Apoiar o desenvolvimento de produtos/serviços com uma base de informação confiável, eficiente e ágil;
- Monitorar analisar e prever questões relacionadas ao "coração" do negócio;
- Gerar valor aos negócios.

Existem várias maneiras de realizar a " inteligência empresarial"

Uma das maneiras de realizar a pesquisa é através do software BI (Business Intelligence), hoje muito utilizados em vários ramos de atividades, como logísticas, Serasa, economia (com a identificação de forças e fraquezas da companhia), investigação de pessoas, tudo vai depender da aplicação e parametrização dos dados, outro software utilizado para investigação é o Otnet.

As organizações tipicamente recolhem informações com a finalidade de avaliar o ambiente empresarial, completando estas informações com pesquisas de marketing, industriais e de mercado, além de análises competitivas, podendo assim mais facilmente intrujar outros.

O conceito surgiu nos Estados Unidos nos anos 90 e refere-se ao processo de coleta, organização, análise, compartilhamento e monitoramento de informações que oferecem suporte a gestão de negócios. É um conjunto de técnicas e ferramentas para auxiliar na transformação de dados brutos em informações significativas e uteis a fim de analisar o negócio ajudando a tomada de decisões.

As organizações tipicamente recolhem informações com a finalidade de avaliar o ambiente empresarial, completando estas informações com pesquisas de marketing, industriais e de mercado, além de análises competitivas, podendo assim mais facilmente intrujar outros.

As atividades consistem em quatro pontos:

- Planejar e identificar as necessidades de informação:

Nesta fase se concebe o processo, seus objetivos e são identificadas as necessidades de inteligência e quais as informações necessárias para atende-las.

- Coletar e tratar a informação: Nesta fase são identificadas as fontes de informações relevantes, internas e externas, e o tipo de tratamento que será dado à informação para armazenamento.
- Analisar e validar a informação: Nesta fase especialista analisam e validam as informações, fazem a sua interpretação e compilam recomendações.
- Disseminar e utilizar a informação: Esta é a fase onde se entrega a informação analisada, ou seja, a inteligência, em um formato coerente e convincente, aos tomadores de decisão.
- Avaliar: Nesta fase a resposta dos tomadores de decisão e suas necessidades de inteligência são analisadas de modo contínuo.

O Bussiness Intelligence também está relacionado ao ERP (Enterprise Resource Planning), que representa os sistemas integrados de gestão empresarial, cuja função é registrar, documentar e processar todas as informações, auxiliando na redução de custos, na otimização do trabalho e principalmente na previsão de crescimento.

A coleta dos dados para tratamento estatístico e as informações decorrentes de sua análise na abordagem constituem-se claramente em atividades de inteligência empresarial. A utilização dessas informações, somadas com outras informações internas e externas à empresa, sobre clientes e concorrentes, pode gerar o conhecimento necessário para a tomada de decisões estratégicas que modificam ou acrescentam ao negócio uma maior capacidade competitiva.

A inteligência empresarial pode ser entendida como uma prática de gestão do conhecimento, com técnicas de execução bastante desenvolvidas.

A gestão do conhecimento atua no desenvolvimento do conhecimento organizacional e no desenvolvimento das competências das pessoas que irão implementar as estratégias das empresas, além de poder tratar e reciclar o conhecimento oriundo da inteligência empresarial para outras finalidades, gerando mais conhecimento.

A inteligência empresarial pode ser entendida como uma prática de gestão do conhecimento, com técnicas de execução bastante desenvolvidas.

"Saber onde encontrar a informação e como usá-la. Esse é o segredo do sucesso".

(Albert Einstein)

PRIMEIRA VEZ EM CURITIBA

SUCESSO EM SÃO PAULO!!

PÓS graduação em GESTÃO de RISCOS CORPORATIVOS

16ª turma

INÍCIO

FEVEREIRO / 2017

b&a
BRASILIANO&ASSOCIADOS
GESTÃO DE RISCOS

conteúdo delhado
www.brasiliano.com.br
ou entre em contato
asilva@brasiliano.com.br

Local - **Slaviero Slim Curitiba**
Endereço - **Rua Conselheiro Araújo, 435 - Alto da XV**

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS
Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano & Associados Gestão de Riscos.
abrasiliano@brasiliano.com.br

O Brasil é vulnerável aos Cyber Riscos. Os gestores de riscos estão preparados?

O Brasil sofre ameaças de uma ampla variedade das chamadas ameaças cibernéticas, inclusive as fraudes virtuais, os crimes cibernéticos e a vigilância digital. Nem todas essas ameaças são por natureza iguais. Indiscutivelmente, o risco mais sério e difundido é o crime virtual de motivação econômica – aquele que visa os bancos privados, firmas e pessoas físicas em busca de proveito.

Outro importante conjunto de ameaças cibernéticas emana de grupos de hackers nacionais e estrangeiros, os quais procuram sabotar serviços governamentais, portais e alvos empresariais. Por exemplo, os maciços protestos populares de junho a agosto de 2013 coincidiram com uma alta no ativismo dos hackers. Por final, as divulgações por Edward Snowden de que as redes oficiais de comunicações do Brasil se sujeitavam à espionagem rotineira pela Agência de Segurança Nacional (NSA) norte-americana, criou o espectro de uma nova ameaça cibernética no país: A ciberespionagem e segundo alguns a ciberguerra. Ao passo que aumenta em todo o Brasil e América Latina a inquietude com as ameaças cibernéticas, conhece-se de fato relativamente pouco sobre as mesmas. Quase não há debates sobre os protagonistas dos quais emanam estas ameaças, seus interesses e motivações, seu modus operandi ou quais suas relações com as mais tradicionais organizações criminosas ou políticas. Há poucos especialistas se ocupando de uma avaliação pormenorizada destas variadas – e até bastante diferenciadas – ameaças cibernéticas, e muito menos ponderando as reações públicas e privadas. Em que pese a profunda falta de conhecimento, mesmo assim o governo brasileiro organizou com rapidez uma abrangente infraestrutura de cibersegurança e defesa. Curiosamente, a resposta possui foco limitado em apenas algumas dimensões destas ameaças – em especial as estrangeiras. Entre as muitas instituições deste meio, o Centro de Defesa Cibernética do Exército Brasileiro (o CDCiber) é peça chave na postura de defesa do país. Até determinado ponto, a aparelhagem de cibersegurança em célere avanço no Brasil, mostra-se em desalinho com as ameaças reais emergentes no ciberespaço. No lugar de mirar com mais precisão o cibercrime internacional e interno, o estado procura uma resposta no aperfeiçoamento da luta contra a ciberguerra e de sua capacidade antiterrorismo. Não significa afirmar que não há perigos nítidos e presentes relativos ao ciberterrorismo e à ciberguerra. Pelo contrário, o presente Estudo Estratégico opina que o governo brasileiro procura uma abordagem de securitização contra as ameaças cibernéticas, no lugar de se contrapor aos desafios mais urgentes em face aos cidadãos, em especial o cibercrime. De forma sucinta, o estado (o agente) securitiza o ciberespaço (o referente) em nome do povo (a plateia).

Ao passo que aumenta em todo o Brasil e América Latina a inquietude com as ameaças cibernéticas, conhece-se de fato relativamente pouco sobre as mesmas.

Definição do ciberespaço brasileiro

O Brasil acha-se sob uma revolução digital com poucos paralelos no mundo em desenvolvimento. O índice de penetração digital e adoção das mídias sociais elevou-se de forma exponencial na

última década. Durante este prazo, o Brasil assistiu a um aumento de dez vezes em acessos à Internet e assinaturas de telefones celulares, constando no presente mais da metade de sua população de 200 milhões conectadas. A quantidade de fatores relativos às melhoras no Brasil do desenvolvimento social e econômico impulsionam estas tendências. O clima macroeconômico, bastante estável, bem como as políticas sociais de redistribuição, levaram à ampliação da classe média no país nos últimos 10 anos. Ao mesmo tempo, a marcha dos novos consumidores motivou a procura por tecnologias de informação e de comunicações (TICs), transformando a escala de suprimento a níveis em conformidade com o vasto mercado interno do Brasil.

A aparição de uma classe média ampliada e conectada dá forma ao ambiente cibernético no Brasil. O acesso mais ágil às novas tecnologias de informações deu causa a uma ampla gama de formas de capacitação social, política e econômica no país. Sem surpresa alguma, a capacitação digital vem acompanhada de maiores desafios a exemplo dos protestos em massa e do crime organizado. Como país de renda mediana, o Brasil se vê obrigado a tratar suas arraigadas desigualdades dentro e fora dos meios digitais. As contradições aparecem à medida em que seus legisladores procuram integrar mais plenamente os cidadãos recém capacitados na democracia e economia formal do país. Como potência emergente, o país se encontra também frente a dilemas com seu maior comprometimento com políticas globais. Logo, fatores internos e internacionais possuem um papel crítico no rumo da governança cibernética do Brasil.

Poucos países foram tão drasticamente afetados pela capacitação digital como o Brasil. A escala e dinamismo do ciberespaço brasileiro atingiu novas alturas nos últimos anos. A começar com as manifestações em massa de inspiração digital, atingindo as ruas do país entre junho e agosto de 2013, até a presença rotineira do mesmo no topo de rankings ativos ao cibercrime. O Brasil é conhecido de modo geral como autor e vítima da criminalidade digital. Ademais, o Brasil ainda se ressente das divulgações de espionagem realizadas por alguns países, em especial os Estados Unidos, Canadá e Reino Unido, tendo iniciado processos de reforma na ONU e internamente. A natureza complexa da "ameaça cibernética" – bem como sua interpretação no Brasil – exerceu um expressivo papel na moldagem da governança cibernética e arquitetura de cibersegurança do país.

Há necessidade de uma avaliação equilibrada ao se considerar as respostas contra as ameaças cibernéticas e a cibersegurança. Torna-se importante levar em conta os poderosos interesses bem como as lutas simbólicas que dão forma à definição do que constitui ameaça digital em determinada sociedade. É possível partir para além do curto prazo em direção à visão de prazo mais amplo que formula as decisões dos grandes protagonistas. Apenas com a adoção da visão bruta será possível compreender por completo o conceito, construção e aplicação da cibersegurança.

Ameaças cibernéticas

Podemos dizer, segundo estudiosos, que há três principais conjuntos de ameaças cibernéticas no Brasil. O quadro abaixo demonstra:

Categoria	Definição	Exemplos	Reações normais do governo	Realidade brasileira
Cibercrime convencional	Trata-se das formas mais difundidas no mundo de infrações cibernéticas, cuja tipologia é a proposta pela ITU (2009) [veja nota de rodapé 4].	Acesso ilícito (cracking), interceptação de dados, pornografia infantil, spam, discurso de ódio, fraude bancária, furto de identidade, infração contra direitos autorais.	Exclusivamente a segurança pública, visto que normalmente compreende crimes tradicionais, já categorizados nos códigos criminais.	Há dois grandes subconjuntos de crimes cibernéticos convencionais: 1) os de motivação econômica (em especial a fraude bancária) e 2) relativos ao conteúdo (por ex: racismo e pornografia infantil nas redes de mídia social).
Cibercrime complexo	Leva em conta e amplia a definição da ITU de infrações cibernéticas complexas ou combinadas, as que se enquadram em mais de uma categoria do cibercrime convencional.	Ciberterrorismo, ciberguerra, ataques contra a infraestrutura crítica, ciberespionagem e ação dos hackers.	Combinação de inteligência, ação militar e segurança pública, visto que há distintas fontes múltiplas e potenciais de ataques (sejam internas ou externas) assim como alvos.	Espionagem comercial e ação dos hackers são duas porém distintas ameaças. Há escassa comprovação de que o Brasil sofra de outros tipos de ameaças nesta categoria.
Ameaças emergentes	Ameaças relativas à expansão do ciberespaço que não se enquadram bem nas categorias da ITU, ou por serem emergentes ou por sua relação com o mundo em desenvolvimento.	TICs empregados pelos mais tradicionais grupos criminais, quadrilhas do crime organizado (drogas e tráfico de armas, extorsão digital, difusão da cultura de violência), ciberlavagem de dinheiro e sonegação fiscal, etc.	Deveria estar mais ligado à segurança pública, porém este campo acaba de emergir e há falta de reação do estado.	O Brasil sofre com os altos níveis de violência interpessoal e organizada, em especial com relação às quadrilhas e o crime organizado que lucra com o tráfico de drogas. Estes já assimilaram o poder das TICs para expandir e fortalecer seus negócios.

No nosso caso iremos abordar com maior foco no Cibercrime convencional, pois é ele que ataca as instituições.

A exemplo das demais atividades ilícitas do mundo real, o cibercrime é extremamente difícil de mensurar com precisão. O ciberespaço é simplesmente enorme e descentralizado demais para aquilatar, acompanhar e relatar com certeza toda a sua atividade dolosa. Com efeito, torna-se bastante difícil até estimar uma ordem de grandeza da cibercriminalidade. Deve-se isto à relutância dos governos e empresas em divulgar este tipo de informação por temor de danos a suas reputações e perda de confiança e investimento. No entanto, algumas agências de estado assim como firmas privadas de cibersegurança emitem relatórios regulares sobre as dimensões estimadas dos mercados da cibercriminalidade. Valores e dados que na melhor hipótese são aproximações brutas, levando a amplas discrepâncias no impacto projetado destes mercados. Não obstante, os mesmos proporcionam alguma visão das grandes tendências capazes de deflagrar a determinação de prioridades assim como as questões sobre a alocação de recursos.

Os relatórios disponíveis apontam para um expressivo aumento da cibercriminalidade no Brasil

no decorrer da década. Tal expansão coincide com o acesso ampliado aos TICs em todo o país a partir do ano 2000. A quantidade total de incidentes cibernéticos recebidos pelo CERT.br (a central do Grupo de Resposta a Incidentes de Segurança em Computadores, ou CSIRT, no Brasil), saltou de 6000 em 2000 para mais de 466.000 em 2012. Pelo menos 75% dos usuários da Internet no Brasil dizem ter sido vítimas de uma ou outra forma de cibercrime. A média global é de 67 por cento, com as maiores taxas localizadas na Rússia (92 por cento), China (84 por cento) e África do Sul (80 por cento). No tocante aos hackers dos perfis das redes sociais, o Brasil encabeça a classe em conjunto com a China, com 23% dos usuários que acusaram a tomada de suas contas por outros usuários. No mínimo 12% dos brasileiros relatam que seus PCs foram infectados por malware através de manobras de phishing por falsos portais transmitidos pela mídia social.

As empresas de cibersegurança também oferecem indicações sobre as dimensões das atividades digitais dolosas no Brasil. De fato, o Brasil consta em primeiro lugar na região da América Latina e Caribe, como fonte e alvo dos ataques digitais. O mesmo vale para toda sorte de infrações cibernéticas cometidas através da informática, a exemplo de códigos maléficos, spam zombies, phishing hosts e botnets, entre outros. Estas tendências grassam a taxas alarmantes. A cibercriminalidade no Brasil evoluiu a passos largos na última década, sendo que as firmas de segurança dos Estados Unidos e da Europa identificaram o Brasil como um dos países mais problemáticos desde 2006 por suas atividades com o cibercrime. Os principais cibercrimes cometidos no Brasil na atualidade incluem a difusão de vírus ou malware (68 %), hacking de perfis na mídia social (19%) assim como o phishing (11%). Embora o Brasil confirme sua grande atividade com spam (3,4% dos fluxos globais em 2012, colocação modesta em comparação com a liderança, EUA com 42,2%), os fluxos vêm decrescendo visivelmente e já não são problema grave entre os usuários.

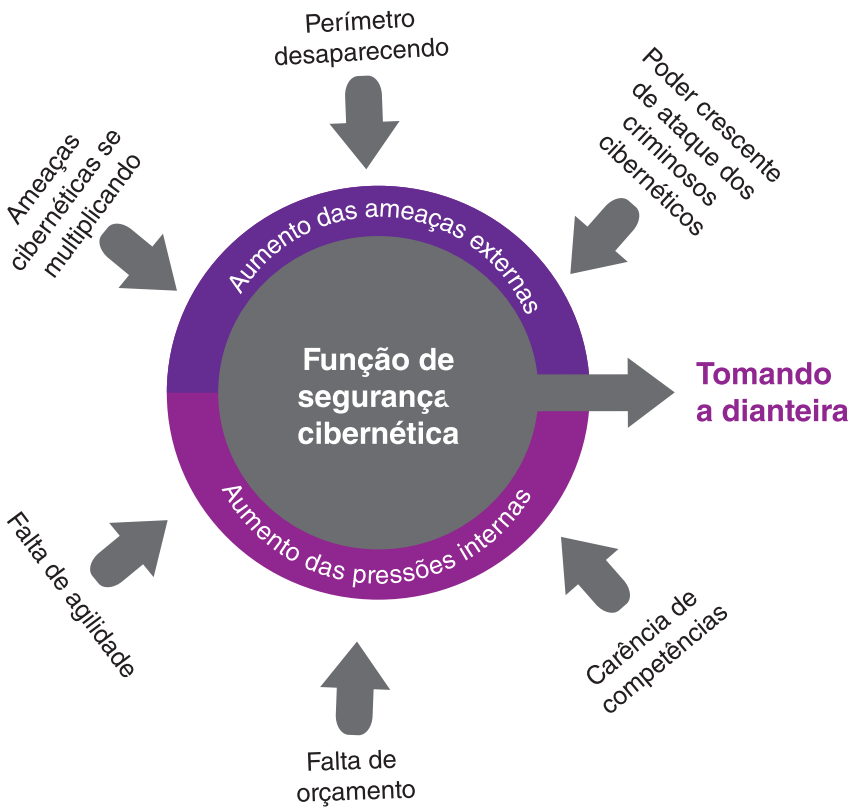
A fraude bancária é quase que uma especialidade no Brasil, em parte por motivo do tamanho do setor de serviços bancários no país.

A Federação Brasileira de Bancos – FEBRABAN relata que as perdas totais das instituições financeiras em 2011 atingiram R$ 750 milhões. A mesma observou também que 60% do incremento anual nas fraudes bancárias ocorreram através da Internet, telefonia móvel, operações das centrais de atendimento e cartões de crédito. Um relatório da Kapersky Labs em 2011 colocou o Brasil na frente da China e da Rússia no emprego do trojan horse para penetrar nas contas bancárias através da rede: 16,9% do total em ataques anuais partiram contra usuários no Brasil, contra 15,8 % na Rússia e 10,8 % na China. Não obstante, grande parte destas fraudes foram perpetradas fora dos meios digitais, através de fraudes com telefones e cartões de crédito (US$ 450 bilhões). Diz-se que foram perdidos US$ 150 milhões através da Internet e do e-banking móvel. Outros US$ 150 milhões foram furtados mediante pagamentos digitais de faturas de cartões de crédito. Em algumas regiões o Brasil supera a América do Norte e a Europa Ocidental em segurança digital do setor bancário: por exemplo, a alteração dos sistemas de senhas, verificação em dois estágios e a biométrica se tornaram padrão.

O Brasil se tornou um porto seguro de outras espécies de cibercrimes identificados pela International Telecommunications Union (ITU). Entre estes, os principais são aqueles perpetrados contra empresas e negócios, relativos a conteúdo assim como infrações contra direitos autorais e marcas registradas. Os custos globais do crime via Internet no Brasil, inclusive fraude e furto de informa- ções bancárias, atinge cerca de US$ 8 bilhões anualmente (ou 7% do total de perdas globais geradas pela cibercriminalidade). Tais estimativas sugerem que o país seja o terceiro mais afetado em todo o mundo pelas atividades digitais ilícitas. O Brasil é de longe o alvo número um na América Latina: O México fica atrás do Brasil com perdas anuais de cerca de US$ 2 bilhões por conta da cibercriminalidade.

Por estes números e cenários é uma obrigação que, nós gestores de riscos, tenhamos ferramentas e processos estruturados para poder de forma direta combater o Cyber Risco, que já é uma realidade. A única forma de enfrentar é manter-se à frente do crime cibernético. Sabemos que enfrentaremos inúmeros obstáculos entre eles a falta de orçamento, falta de agilidade da alta gestão em compreender a problemática, carência de competências – capacitações, poder crescente dos ataques dos criminosos, perímetro de segurança cada vez mais esgarçado para o crime cibernético e as ameaças cada vez mais se multiplicando. Mas mesmo assim o Gestor de Risco deve acreditar em processos estruturados e em metodologias e ferramentas para podermos de fato enfrentarmos a Cibernética como deve ser.

O diagrama ao lado demonstra que o poder dos criminosos cibernéticos está aumentando, e as organizações lutam contra inúmeros obstáculos.



A postura tem que ser ativando os chamados três A's: Ativar, Adaptar e Antecipar.

Cada organização necessita de uma base sólida de segurança cibernética. Concretizá-la não é uma tarefa fácil, e as especificações das necessidades vão depender de questões como o setor de atividade e a localização geográfica. Esses fundamentos proporcionam o primeiro passo na jornada de segurança cibernética.

Cabe a nós, gestores de riscos começarmos a dar o primeiro passo!

Você já inclui na agenda de 2017 a disciplina de Riscos Cibernéticos no seu portfólio de riscos? Espero que sim!!

Comemorando nossos 28 anos, solicite gratuitamente para o email mgoncalves@brasiliano.com.br o novo livro digital **Inteligência em Riscos.**

BOA LEITURA!

ler e saber

CURSOS ONLINE

otimize seu tempo

adquira no site www.sicurezzaeditora.com.br

REVISTA
GESTÃO DE RISCOS

b&a BRASILIANO & ASSOCIADOS
EDIÇÃO 103
NOVEMBRO 2016

Críticas e sugestões de pauta:
revista@brasiliano.com.br

www.brasiliano.com.br

Publisher: Antonio Celso Ribeiro Brasiliano

Edição: Enza Cirelli

Coedição: Matheus Fridori

Edição de arte: Marina Brasiliano

Edição 103 - Novembro 2016 | 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