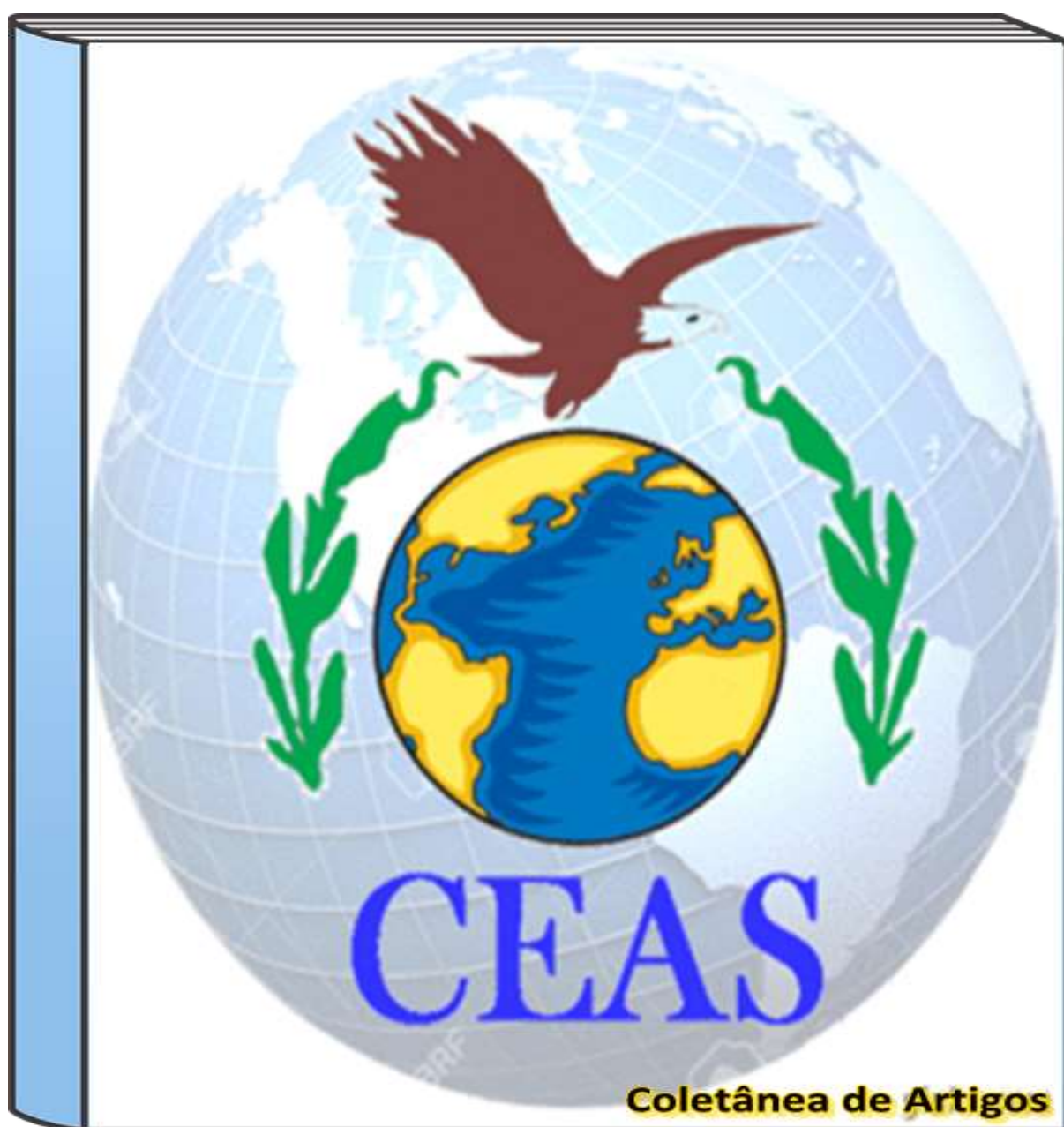




Edição II

2019

INTRODUÇÃO

As organizações estão inseridas em um ambiente altamente competitivo. Esta realidade obriga as empresas a serem eficazes, eficientes e efetivas. Os lucros estão cada vez menores e o preço de seus produtos e/ou serviços são ditados pelo mercado. Para que as margens de lucro sejam compatíveis com as suas necessidades, as organizações precisam melhorar os seus processos e nesta busca o gerenciamento de risco é fundamental. Além desta vertente empresarial, outro ponto tem afetado o sucesso das organizações, o aumento da criminalidade. Aumento este, decorrente de uma série de fatores, dentre eles a falência do Sistema Público de Segurança. A soma de fatores empresariais e públicos tem potencializado a importância da Segurança Empresarial na obtenção do sucesso corporativo. Com esta potencialização, fez surgir a necessidade de departamentos de segurança com atuação científica, ou seja, não se admite mais o empirismo ou o “achismo” nas ações de segurança. Este contexto fez elevar o nível da prestação de serviços terceirizados de segurança ou de sistemas orgânicos de segurança. Para gerir o Sistema de Segurança é necessário um profissional altamente qualificado. Uma pessoa que gerencie de forma científica. Que saiba interagir a teoria com a prática. Alguém que tenha as competências (conhecimento, habilidade e comportamento) necessárias para ajudar a empresa a ser altamente competitiva. Esta necessidade criou a base para o surgimento dos cursos de graduação e pós-graduação na área de Segurança Empresarial. Cursos que são multidisciplinares e focados na prática. Mas para que os cursos cumpram com a sua missão é fundamental a existência de fontes de consulta. Não existe nenhuma dificuldade para a aquisição ou consulta de livros, dvds e periódicos nas áreas de engenharia, administração, direito, psicologia, ética, comunicação, economia, dentre outras. O mesmo não acontece com a área de segurança. Não podemos negar que já temos alguns livros, dvds e períodos, mas não na quantidade e qualidade que a evolução do segmento necessita.

Baseado no exposto acima, é que estamos lançando este trabalho. Uma coletânea de artigos que busca dotar os gestores dos conhecimentos necessários para serem capazes de fazer uma gestão científica e alinhada com a estratégia da empresa. Não queremos afirmar que os assuntos abordados nos diversos artigos estão esgotados, mas pontos importantes foram abordados. Além de abordarmos os pontos principais, temos o objetivo de despertar nos leitores a percepção da importância de aprofundamento dos diversos temas. São artigos produzidos por nossos sócios. Desejamos aos leitores uma ótima leitura e muito sucesso na gestão dos seus departamentos ou empresas.

AS FALHAS E A GESTÃO DE RISCOS

Uma situação de falha ocorre quando um componente (homem ou equipamento) de um sistema executa uma função de forma inadequada ou deixa de executá-la. As falhas são fatores de risco e na quase totalidade dos casos, os eventos ocorrem devido a algum tipo de falha. Grande parte da gestão de riscos consiste em identificar possibilidades de falha e adotar medidas para minimizá-las, reduzindo a probabilidade e ou o impacto.

A análise das falhas consiste em identificar: o modo e o tipo da falha; os agentes promotores e inibidores; a fase do ciclo de vida do componente ou o sistema em que a falha ocorreu e a fase geradora.

Um componente pode falhar de cinco maneiras: omissão, missão, ato estranho, sequencial e temporal. A falha de omissão ocorre quando o componente não executa ou executa parcialmente uma função. Tanto o meio humano quanto os meios técnicos (ativo e passivo) são passíveis deste tipo de falha. Em relação ao meio humano, o subsistema de normas e procedimentos e o treinamento contribuem para minimizar. Já em relação aos meios técnicos, o que minimizará é o planejamento tático e técnico.

A falha é na missão quando o componente executa incorretamente uma função. Esta falha é minimizada com a gestão eficiente e eficaz do meio humano. Já a falha por ato estranho ocorre quando o componente executa uma função que não deveria ter sido executada.

O quarto modo, falha sequencial, ocorre quando o componente executa uma função fora da sequência correta. Enquanto que na falha temporal, o componente executa uma função fora do momento correto. Nestes dois últimos modos, o planejamento (tático, técnico e operacional) e a gestão eficiente e eficaz do meio humano são capazes de minimizar.

Falha do meio humano

No conjunto das falhas, a falha do meio humano está em destaque. Classifica-se este tipo de falha em: técnica, descuido e consciente. A falha será técnica quando cometida por falta de meios adequados para exercer a função. Os recursos inexistem ou são inadequados ou a relação homem-sistema (ergonomia) não é adequada. O ser humano falha porque não sabe ou não pode fazer da maneira correta.

A falha é por descuido (inadvertência ou inconsciente) quando decorre da incapacidade dos mecanismos inconscientes e automáticos em controlar ações da pessoa. O ser humano tem todos os recursos e atua corretamente em grande número de vezes, mas esporadicamente ele falha. As características básicas são: esporádica e baixa probabilidade.

As falhas por descuido são ampliadas pela desatenção inerente às situações de baixa tensão, bem como pela confusão das situações de alta tensão. Não podemos esquecer que o ser humano tem dificuldade em manter a atenção contínua por longos períodos, logo quanto mais o sistema depender dessa atenção para operar com segurança, maior a probabilidade de falhas (exemplo: operador de central de monitoramento de imagens). Nas condições de rotina duas situações concorrem para deteriorar a atenção: monitoramento contínuo e tarefas repetitivas.

Falha consciente é a falha provocada pela adoção de procedimentos alternativos que envolvem maiores riscos que o procedimento padrão. Diante da possibilidade de optar entre dois procedimentos, o ser humano entra em conflito e a decisão dependerá do balanço das forças que atuam no sentido do padrão e do alternativo.

Falha de equipamento

Existem três tipos de falha: T, D e C. A falha T ocorre quando o equipamento não é capaz de exercer a missão requerida. Pode ocorrer nos seguintes casos: equipamento não está projetado para a função; as condições de trabalho são diferentes das de projeto e equipamento está em um estado falho.

Na falha tipo D, o equipamento tem capacidade para exercer a função e a exerce bem na maior parte do tempo, mas falha esporadicamente. Pode ocorrer nos seguintes casos: equipamento tem componentes cujas falhas não se manifestam de forma permanente e alguma condição de trabalho varia de forma esporádica.

Na falha C o equipamento tem capacidade para exercer a função, mas sistematicamente exerce de modo falho. São falhas C as decorrentes de ajustes incorretos de sistemas de comando.

Agentes promotores

Qualquer falha da pessoa ou de equipamento é promovida por agentes promotores. Existem quatro agentes: primário, secundário, comando e intruso. A falha primária é a que ocorre no ambiente e sob carga para as quais o componente é qualificado. Geralmente são provocadas por projeto, fabricação ou construção, envelhecimento ou falha de manutenção. A falha primária do ser humano ocorre quando ele é ou se torna incapaz de desempenhar a função de projeto sob condições de projeto.

A falha promovida por agente secundário é a que ocorre em um ambiente e sob carga para a qual o componente não é qualificado. O ser humano comete este tipo de falha quando trabalha sob condições adversas, como layout inadequado, calor, ruído, horas extras e tensões psicológicas externas.

Falha promovida por agente comando é a que ocorre quando o componente atua incorretamente obedecendo a algum elemento do sistema. O ser humano comete este tipo de falha sob comando de superiores, procedimentos e cultura. A falha por comando é promovida por uma informação.

Muitas vezes o ser humano atua como intruso e provoca falha no sistema, podendo, inclusive, desativar dispositivos dos quais depende o controle ou a proteção. Podemos considerar agente intruso tudo que for estranho ao sistema ou ambiente normal.

Prof. Dr. Nino Ricardo de Menezes Meireles, CPSI,DIDS,CIGR,CIEIE

Doutor em Ciencias de La Seguridad (Espanha).Coordenador MBA em Gestão Estratégica da Segurança - Faculdade Einstein (FACEI). Docente e Diretor de Formação e de Extensão Universitária da Corporación Euro Americana de Seguridad, Capítulo Brasil e Autor de 8 livros.

COMPLIANCE NAS ORGANIZAÇÕES

A origem da palavra compliance verbo em inglês to comply que significa: cumprir, obedecer ou atender. A expressão é usada com o significado de estarem conformidade com regras, legislação e normas.

Risco de compliance é definido como risco legal, ou de sanções regulatórias, de perda financeira ou de reputação que uma empresa pode sofrer como resultado de falhas no cumprimento de leis, regulamentações, códigos de conduta e das boas práticas entre organizações. Para entender perda de reputação deve-se partir do pressuposto que essa se baseia na síntese de como os clientes, funcionários e acionistas veem a organização. As principais subáreas são: risco de legislação, risco de contrato e risco tributário.

Compliance é uma questão de ética. O programa de compliance deve auxiliar funcionários na resolução de situações não cobertas pela legislação e tem dois objetivos: prevenir a ocorrência de infrações e demonstrar a eficácia dos controles. É importante saber quais normativas e leis são aplicáveis à empresa e qual a melhor maneira de se ajustar a elas e cumpri-las.

Programas voltados à boa conduta e programas de compliance devem estar integrados, pois se baseiam em valores e responsabilidade morais, bem como no cumprimento e conformidade das leis e políticas internas. Em uma economia em que 70% a 80% do valor do mercado vêm de ativos intangíveis de difícil avaliação (valor da marca, capital intelectual), a empresa torna-se vulnerável a tudo que possa prejudicar sua reputação.

SISTEMA DE COMPLIANCE

PREVENIR

- **Gestão de riscos de compliance** - Análise das operações da empresa com o objetivo de detectar os riscos de compliance e introdução de medidas para minimizar os riscos são os elementos chaves.
- **Políticas e procedimentos** - O código de conduta é o elemento chave do sistema de compliance. Nele se definem as normas de conduta essenciais.
- **Formação e comunicação** - As normativas são ineficazes se os colaboradores não as conhecem e não sabem como por em prática. Um dos elementos chaves para a implantação do sistema de compliance é a formação.
- **Conselho e apoio** - Dar conselho e apoiar as unidades de negócio é uma das funções principais do sistema de compliance.
- **Coletividade** - Uma empresa sozinha pode lograr resultados limitados na luta contra a corrupção. Para obter avanços substanciais é necessária uma atuação conjunta de todos ou ao menos, do maior número possível de participantes do mercado.

DETECTAR

- **Canais de denúncia** - Dispor de canais de denúncia e proteção ante possíveis sanções de colaboradores que informam sobre possíveis condutas indevidas.
- **Controles** - Com o objetivo de elevar a eficiência do sistema de compliance deve-se implantar um conjunto de controles que inclui tanto controles anticorrupção como controles antifraude.
- **Revisão** - O sistema deve ser avaliado permanentemente para poder localizar melhorias.
- **Auditorias** - Revisão periódica da implantação do Compliance Control Framework.
- **Investigações** - Processo de investigação dotado de recursos para analisar as possíveis infrações de compliance.

GESTOR DE COMPLIANCE

Responsável por saber que normativa(s) e lei(s) são aplicáveis à empresa e qual é a melhor maneira de ajustar-se a elas e as cumprir. Deve ter conhecimento amplo de leis e normas. Recomendável que conte com ampla experiência em assessorias jurídicas e/ou fiscais.

Deve ter expertise na definição e implementação de planos de compliance e no uso de metodologias e ferramentas que facilitam e agilizam seu trabalho.

MÉTODO

Definir objetivos

A Norma ISO 19600:2015 é uma referência aplicável a qualquer empresa e oferece as diretrizes para implementar, avaliar, manter e melhorar um sistema de compliance.

Acompanhar mediante indicadores

Verificar se os objetivos de compliance estão sendo alcançados. Permite ao gestor de compliance saber qual é o nível de risco atual, comunicá-lo à direção e desenvolver um plano de melhorias.

Utilizar métodos de análise de riscos

Com o objetivo de detectar os riscos de compliance e introduzir medidas apropriadas para a minimização de riscos. Analisar e avaliar os riscos segundo seu impacto e sua probabilidade mediante alguma metodologia.

Monitorar

Toda a informação gerada deve ser rastreada.

Gerar evidências

No caso de se cometer alguma infração, um bom programa de compliance deve estar desenvolvido de maneira que possa demonstrar que existiam controles para evitá-lo e que estes eram eficazes.

Segregar funções

Para evitar que uma única pessoa ou um único departamento leve a cabo tarefas incompatíveis que possam dar lugar a fraude, é recomendável segregar funções.

Elaborar um código de ética

É recomendável criar um Código de Ética e distribuí-lo para todos os departamentos.

Canal de denúncia

Para investigar casos de fraude, é importante existir um canal de denúncia (interno e externo), de forma que tanto colaboradores como clientes, fornecedores ou outros grupos de interesse possam denunciar condutas contrárias ao Código de Ética por parte de um colaborador ou um departamento.

Prof. Dr. Nino Ricardo de Menezes Meireles, CPSI,DIDS,CIGR,CIEIE

Doutor em Ciencias de La Seguridad (Espanha).Coordenador MBA em Gestão Estratégica da Segurança - Faculdade Einstein (FACEI). Docente e Diretor de Formação e de Extensão Universitária da Corporación Euro Americana de Seguridad, Capítulo Brasil e Autor de 8 livros.

CEAS

ESTUDO DAS TERMINOLOGIAS: VIGILANTE E VIGIA

São muito comuns, no meio dos profissionais de segurança patrimonial privada, as divergências no entendimento dos termos vigilante e vigia. Alguns defendem a ideia de que ambas as terminologias apresentam a mesma significação, como se fossem expressões sinonímicas, e outros postulam que há uma distinção: vigilante é o termo utilizado para se referir aos profissionais que desempenham as funções descritas no Art. 10 da lei nº 7.102, de 20 de junho de 1983, enquanto vigia refere-se ao profissional que desempenha funções de porteiro.

O dicionário *Aurélio* define o termo vigia como “*ato ou efeito de vigiar*”, vigiar (Do latim *vigilare*) como “*observar atentamente*”, informando que vigiar é um verbo transitivo direto, e vigilante (Do latim *vigilante*) como aquele “*que vigia*”. Assim sendo, o termo vigia é uma função, e vigilante é aquele que desempenha as funções de vigia, pela ação de vigiar.

O Código Brasileiro de Ocupações – CBO do Ministério do Trabalho – MT esclarece o termo vigilante na família número 5173: “Vigilantes e guardas de segurança”, descrevendo as funções dessa atividade, como:

“Vigiam dependências e áreas públicas e privadas com a finalidade de prevenir, controlar e combater delitos como porte ilícito de armas e munições e outras irregularidades; zelam pela segurança das pessoas, do patrimônio e pelo cumprimento das leis e regulamentos; recebem e controlam a movimentação de pessoas em áreas de acesso livre e restrito; fiscalizam pessoas, cargas e patrimônio; escoltam pessoas e mercadorias. Controlam objetos e cargas; vigiam parques e reservas florestais, combatendo inclusive focos de incêndio; vigiam presos. Comunicam-se via rádio ou telefone e prestam informações ao público e aos órgãos competentes”. (grifo meu).

Assim sendo, o termo vigiar, aqui descrito pelo Ministério do Trabalho – MT, tem tido o mesmo entendimento encontrado no dicionário *Aurélio*-, pois ambos entendem que a finalidade principal de vigiar é cuidar da integridade da vida e de bens.

O CBO descreve também as funções de “vigia/porteiro” na classe 5174:

“Recebem e orientam visitantes e hóspedes. Zelam pela guarda do patrimônio observando o comportamento e movimentação de pessoas para prevenir perdas, evitar incêndios, acidentes e outras anormalidades. Controlam o fluxo de pessoas e veículos identificando-os e encaminhando-os aos locais desejados...”. (grifo meu).

Assim sendo, para efeitos do Código Brasileiro de Ocupações – CBO, os termos vigia, guarda e vigilante têm o mesmo sentido, que é o de zelar pelo patrimônio de pessoas e ou de bens.

No entanto, no inciso I do parágrafo 3º do artigo 1º da Portaria nº 3.233/2012-DG/DPF, de 10 de dezembro de 2012, assim se descrevem as duas funções básicas da atividade de vigilância:

“§ 3º São consideradas atividades de segurança privada:

I - vigilância patrimonial: atividade exercida em eventos sociais e dentro de estabelecimentos, urbanos ou rurais, públicos ou privados, com a finalidade de garantir a incolumidade física das pessoas e a integridade do patrimônio”; (o grifo meu)

Percebemos que a finalidade do vigilante é a de zelar pelo patrimônio de pessoas e ou de bens e que, em suas atribuições, são realizadas as atividades de vigiar ou observar o patrimônio, bem como outras atividades para manter a incolumidade de pessoas e bens.

O Poder Judiciário também entende desta forma, pois os Juízes da Justiça do Trabalho defendem uma diferenciação entre “vigia” e “vigilante”, descrevendo que a função de vigilante corre perigo de vida do profissional, como vimos a seguir:

“Segundo o magistério de Valentin Carrion, “... vigilante é o empregado contratado para proceder à vigilância patrimonial das instituições financeiras e de outros estabelecimentos, públicos ou privados”, ao passo que “vigia é o que exerce tarefas de observação e fiscalização do local, sem os requisitos formais, estritos dos vigilantes. Seus direitos são os comuns dos trabalhadores urbanos”.

Fonte: TRT-1 - Recurso Ordinário: RO 1275000720095010511 RJ.

Disponível em:

<https://trt1.jusbrasil.com.br/jurisprudencia/24932196/recurso-ordinario-ro-1275000720095010511-rj-trt-1>

A interpretação jurífica também corrobora com a mesma linha de entendimento sobre a diferenciação dessas funções:

“ [...] Tal função é definida pela doutrina e jurisprudência como sendo mais passiva do que aquela exercida pelo vigilante, esta mais caracterizada como uma função policial privada (para policial), de natureza tanto preventiva como repressiva, característica esta, de repressão, que não se coaduna com a atividade de “vigia”, “porteiro”, “ronda”, da qual não se exige preparação especial, tampouco que atue ou reaja contra atos de outrem contra a vida ou patrimônio de seu empregador. [...] (8ª Turma. Relator o Exmo. Desembargador João Paulo Lucena. Processo n. 0020811-39.2015.5.04.0221 RO. Publicação em 21-07-2017)”.

Percebemos que o Judiciário e o legislativo têm o mesmo entendimento quanto ao termo vigia e vigilante, ou seja, estas palavras se tornaram expressões sinônimas, algo bem provável porque **se tornou um senso comum** amplamente aceito por todos, “convencionou-se” que vigilante é aquele que desempenha as funções previstas na Lei 7.102 e Portaria 3.233, “que atue e reaja”, mas de forma ativa, enquanto que vigia é aquele que

desempenha as funções de porteiro, *“da qual não se exige preparação especial, tampouco que atue ou reaja contra atos de outrem contra a vida ou patrimônio de seu empregador”*.

É urgente a distinção destes termos, pois, se já é confuso para os profissionais da área de segurança, é ainda mais para os demais, como os clientes que contratam estes serviços, os quais podem acabar contratando vigia, pensando que os serviços serão de vigilante. Além disso, há algumas empresas que não são especializadas em vigilância privada e que não têm autorização de funcionamento da Polícia Federal para exercerem funções de vigilância, ademais há aquelas que não estão sob a lei 7.102 e que podem induzir o cliente ao erro, fazendo acreditar que, por contratar os serviços de vigia, terão serviços de vigilância privada focados em cuidar e combater para garantir a segurança de pessoas e de patrimônio.

Cabe ressaltar que o piso salarial de vigia é menor e não incide periculosidade de 30%, como o de vigilante, o que já sinaliza para uma diferenciação das funções, algo que precisa estar claro para empresas e clientes. Outro fator que dificulta ao entendimento do cliente é o uniforme, cujas características são semelhantes: aqueles que contratam serviços de “vigia”, ao ver o colaborador fardado como um para-militar semelhante ao vigilante, acreditam se tratar de um vigilante privado.

A distinção dos termos vigia e vigilante deve ser considerada inicialmente para normatizar os serviços de vigilância privada, distinguindo dos serviços exercidos por porteiros ou recepcionistas cujas atribuições são os processos relacionados de atendimento ao público interno e externo, controlar acessos, controles de chaves, fazer cumprir normas e procedimentos e registros e comunicação de ocorrências, identificação e comunicação de riscos. É preciso ter clareza de que os serviços de vigilância caracterizam-se pelas ações ativas em agir para zelar e proteger as pessoas e bens *“que atue e reaja”*, bem como para combater. Neste sentido é um requisito o treinamento em Centros de Formação de Vigilância autorizados e fiscalizados pela Polícia Federal, nos quais, entre as disciplinas ministradas, estão o uso progressivo da força, gerenciamento de crises, defesa pessoal, armamento e tiro, armas não letais, sistema nacional de segurança pública e crime organizado, noções de vigilância, primeiros socorros, combate a incêndios, entre outras. Em suma, o vigilante é treinado para identificar, mitigar e combater os riscos, enquanto que vigia/porteiro apenas identifica e comunica os riscos, além de outras atribuições, como de atendimento ao público, orientações e registros.

Uma empresa que oferta serviços de vigia pode prejudicar a comercialização dos serviços de uma empresa de vigilância privada, pois o serviço de vigia, além de ter um custo menor, não é o mesmo que o de vigilância, é mais “limitado”. Não havendo essa clareza entre esses dois serviços, pode-se incorrer na compra de um serviço que, de fato, não será ofertado, porém será de menor valor ao contratante.

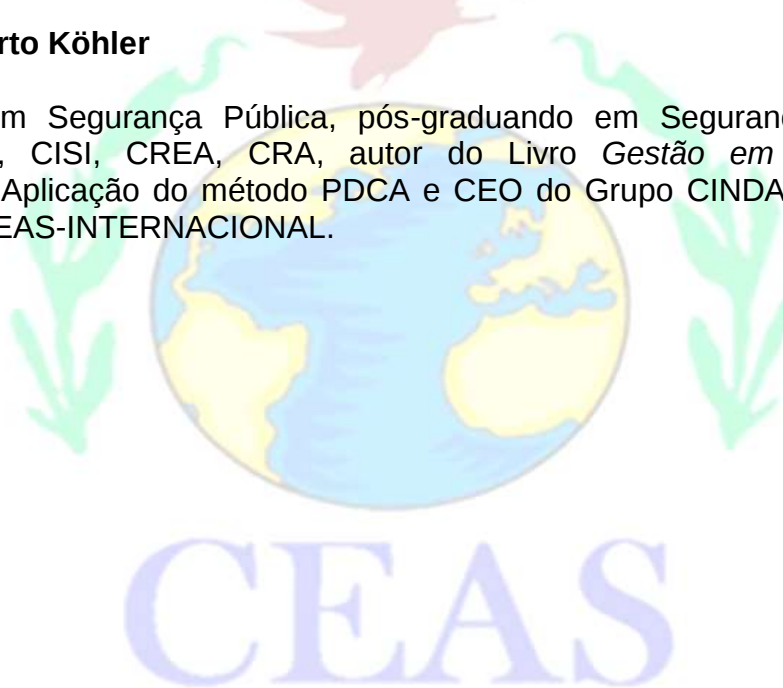
Diante do exposto, não restam dúvidas de que é necessário adequar o termo “vigia” para outro termo como porteiro, ou ainda outro a ser amplamente debatido, ou normatizar estas expressões aparentemente sinonímicas, bem como realizar a atualização dos termos e funções no CBO.

Referências

- BRASIL. (s.d.). LEI Nº 7.102, DE 20 DE JUNHO DE 1983. BRASIL.
- BRASIL. (s.d.). *MINISTÉRIO DO TRABALHO E EMPREGO*. Fonte: MINISTÉRIO DO TRABALHO E EMPREGO: <http://www.mtecbo.gov.br/cbosite/pages/pesquisas/BuscaPorTituloResultado.jsf>
- BRASIL. (s.d.). PORTARIA Nº 3.233/2012-DG/DPF, DE 10 DE DEZEMBRO DE 2012. BRASIL.
- BRASIL. (s.d.). *TRT - Recurso Ordinário: RO 1275000720095010511*. Acesso em 13 de Fevereiro de 2018, disponível em TRT: <https://trt-1.jusbrasil.com.br/jurisprudencia/24932196/recurso-ordinario-ro-1275000720095010511-rj-trt-1>
- Brasil, T. R. (2017). ATIVIDADES PROFISSIONAIS DE SEGURANÇA. *Revista Eletrônica: Acórdãos, Sentenças, Ementas, Artigos e Informações*. Acesso em 10 de Março de 2018, disponível em <file:///C:/Users/Carlos%20Kohler/Downloads/207edicao.pdf>
- FERREIRA, A. B. (2004). *NOVO DICIONÁRIO AURÉLIO DA LINGUA PORTUGUESA*. Curitiba, Paraná, Brasil: Positivo.

Carlos Alberto Köhler

Graduado em Segurança Pública, pós-graduando em Segurança Privada, MBS, CPSI, CISI, CREA, CRA, autor do Livro *Gestão em Segurança Patrimonial: Aplicação do método PDCA e CEO do Grupo CINDAPA* e Sócio Honorário CEAS-INTERNACIONAL.



TEORIA DO CRIME

Triângulo do crime – Dinâmica no cenário shopping center

O primeiro centro de compras do país foi inaugurado em 1966 e, num primeiro momento, causou desconfiança em empresários e investidores pelo formato fechado, conflitando com o badalado e luxuoso comércio de rua que predominava na época. Com o tempo a disputa pelos melhores espaços provou que os visionários empreendedores estavam certos em sua aposta, pois logo o empreendimento se transformou num importante ponto de encontro da cidade de São Paulo. Mais de cinquenta anos se passaram e este modelo de centro de compras sofreu grandes mudanças conceituais ao longo de todos estes anos, se transformando nos grandes locais de entretenimento que vemos hoje.

Os shopping centers são estruturas pensadas e construídas para receber grandes quantidades de pessoas que buscam, em sua grande maioria, um ambiente confortável, climatizado, limpo, seguro, com ótimo atendimento desde sua entrada e que ali possam resolver tudo com total segurança. Segundo dados da **ABRASCE – Associação Brasileira de Shopping Centers** – temos hoje no Brasil 571 empreendimentos e outros tantos em construção que recebem mensalmente mais de 400 milhões de clientes passando pelos corredores destes espaços confiantes que estão sendo muito bem cuidados. Essa é a percepção dos clientes.

Por ser considerado um local seguro muitos empresários do segmento joias e relojoarias que possuíam lojas de rua optaram em locar espaços dentro destes grandes empreendimentos onde podiam atender um público muito exigente de forma diferenciada, discreta e segura. Este era o cenário...

Ocorre que, os shoppings passaram a ser alvo de constantes ataques de quadrilhas bem organizadas e articuladas cujo foco principal são produtos de fácil negociação como relógios, joias e aparelhos telefônicos, situação que mudou completamente o cenário anterior. As ações criminosas, cada vez mais ousadas, têm se mostrado recorrentes em alguns empreendimentos, deixando algumas dúvidas, a saber:

- 1) Por que as ações criminosas se voltaram para os shoppings?**
- 2) Quais os critérios adotados pelos criminosos para escolher um alvo específico?**
- 3) Por que não se consegue dar uma resposta assertiva de modo a inibir atos criminosos?**
- 4) Por que determinado empreendimento sofre com mais ataques que outro, situado no mesmo bairro?**

Essas perguntas só podem ser respondidas se deixarmos de lado o modelo mental ultrapassado que tipifica um criminoso como alguém sem estudo, com baixo nível intelectual e cultural e que seja incapaz de articular com outros elementos em prol de um objetivo delituoso que gere benefícios para todos os envolvidos.

Isso mesmo. Esse modelo dominante nos fez imaginar que o shopping fosse algo intransponível enquanto deixamos de considerar ainda outro importante fato. A sazonalidade das ações criminosas. Exatamente isso. Basta analisar os dados estatísticos dos últimos anos e podemos observar

claramente que existe uma mudança no foco das ações nos diferentes períodos da história recente.

Sem a necessidade de ser específico com datas, pois a temática abordada no estudo é o cenário shopping center, observamos que, ao longo dos últimos vinte e cinco anos, as ações criminosas de grande vulto contemplaram as seguintes modalidades:

- Assalto a agências bancárias;
- Sequestro e sequestro relâmpago;
- Assaltos a casas lotéricas;
- Explosões de caixas eletrônicos;
- Assaltos a shoppings e
- Roubo de cargas.

Não consideramos nesta lista o tráfico de drogas pelo simples fato que este apresenta uma característica atemporal, ou seja, sempre existiu neste período independente das outras ocorrências e dos impactos causados por cada tipo criminal.

Comprovadamente os tipos criminais mudaram ao longo dos anos assim como os objetivos e isto exigiu por parte dos infratores certa perspicácia e um nível de inteligência capaz de identificar as VULNERABILIDADES em cada alvo potencial.

As percepções deste breve estudo foram compartilhadas com cinco gestores de grandes administradoras do varejo Brasileiro e, excetuando-se pequenas divergências sobre os fatores externos e de localização do empreendimento, as conclusões uníssonas serviram de base para as respostas das perguntas feitas na introdução do estudo.

1) Por que as ações criminosas se voltaram para os shoppings?

Os produtos de fácil repasse como celulares, joias, relógios e dinheiro (Casa de câmbio e lotéricas) dentro de um ambiente vulnerável que não possibilita reação em razão dos impactos que esta pode causar. Algumas administradoras optam em ter agentes desarmados.

2) Quais os critérios adotados pelos criminosos para escolher um alvo específico?

Os criminosos planejam muito bem suas ações e, durante as várias visitas a diferentes empreendimentos, escolhem aquele que apresentar maior vulnerabilidade, facilidade de acesso e saída. Este será fatalmente um alvo potencial. Rotas de fuga difíceis e proximidade de órgão públicos podem ser inibidores de ações em locais bem específicos.

3) Por que não se consegue dar uma resposta assertiva de modo a inibir atos criminosos?

Para que uma resposta seja assertiva uma combinação de protocolos operacionais e técnicos devem ser implantados, para isso é necessário que o empreendimento disponha de um aparato tecnológico (meios técnicos ativos) que permita a rápida identificação de suspeitos, ou seja, um sistema de monitoramento capaz de apoiar a

confirmação de um rosto ou comportamento que denote ação iminente. As equipes de segurança devem passar por treinamentos que ainda não são considerados em sua forma ampla nos cursos técnicos. Avaliar comportamentos, por exemplo, deve ser uma das matérias obrigatórias para quem atua na área, afinal um shopping é aberto ao público durante todo o dia e como identificar que uma ação está em curso...? Alguns empreendimentos recebem milhares de pessoas e como saber quais vão cometer um ato ilícito...?

4) Por que determinado empreendimento sofre com mais ataques que outro, situado no mesmo bairro?

Simples. Se os criminosos estudam sistematicamente os ambientes é logico que irão optar pelo que se encontrar mais vulnerável. Temos casos em que existem dois shoppings muito próximos, mas apenas um vira alvo recorrente de ações, justamente pelo fato de ser encontrado em maior estado de vulnerabilidade que o outro.

Aprofundado a questão das vulnerabilidades, adaptamos o triângulo do crime para o cenário shopping center de modo a criar uma interface entre os critérios observados para consumação de um fato criminal e as variáveis do ambiente interno de um empreendimento. Basta um olhar mais técnico e criterioso sobre as nuances do cenário e a relação sistêmica da teoria do crime, de certo teremos corroboradas todas as assertivas dos colegas gestores na figura ilustrativa. Vejamos.



A teoria do TRIANGULO DO CRIME pressupõe a prevalência de três variáveis para que um ato criminoso ocorra:

a) O indivíduo motivado

A obtenção de algo que despertou desejo.

Dentro de um shopping temos ótimos atrativos de fácil negociação e ainda dinheiro em espécie, nas casas lotéricas, casas de câmbio e agências bancárias. Tudo num único lugar.

b) O emprego de técnica

O elemento precisa dominar conhecimento suficiente para ter êxito no seu intento.

O que se confirma após a investigação interna pós crime é que os autores empreenderam várias “visitas técnicas” a fim de estudar o local, planejar a ação para poder executar o objetivo, ou seja, todas as vulnerabilidades foram consideradas antes da decisão final dos criminosos.

c) A oportunidade

O momento (cenário) mais favorável para a consumação do ato.

Após estudar todas as possibilidades dentro de um empreendimento os elementos ainda necessitam de um cenário bem específico. Trata-se de uma combinação de fatores de risco que podem ocorrer em diferentes momentos ou em um único momento, proporcionando uma “janela” facilitadora da concretização da prática criminosa.

A consumação de um fato criminoso, em mais 70% dos casos, se concretiza por falha ocorrida dentro do sistema preventivo de segurança, ou seja, o criminoso explorou alguma das vulnerabilidades observadas no empreendimento e o escolheu como alvo para realizar seu objetivo.

Segundo BRASILIANO (2010, p. 42) a identificação dos perigos e de seus fatores significa a compreensão das origens de cada perigo. Deve-se buscar responder por que o perigo existe na empresa. Quais são as condições que potencializam a concretização do evento estudado.

A compreensão da origem do perigo é imperiosa para a eficácia no tratamento, na priorização que a empresa vai poder dedicar para mitigar aquela situação. Somente após o entendimento do porquê da existência de cada perigo, é que se poderá sugerir medidas eficazes para reduzir riscos.

O DIAGRAMA DE ISHIKAWA (causa e efeito) é a ferramenta que permite a organização identificar, dentro do contexto da GESTÃO DE RISCOS, quais são os facilitadores na materialização dos riscos e preparar suas defesas, através de um plano de ação.



Dentro do cenário shopping center, no que tange as variáveis contempladas no DIAGRAMA, cabem algumas considerações:

- 1) Um empreendimento que foi projetado para receber milhares de pessoas por dia deve possuir um sistema de gerenciamento de riscos bem consolidado e atualizado conforme cenários;
- 2) No planejamento de segurança a aplicação dos investimentos deve observar o equilíbrio entre recursos humanos e toda a gama de treinamentos e tecnológicos (segurança física e segurança eletrônica). Ambos são complementares e, neste cenário, um não vive sem o outro;
- 3) A questão do recrutamento das equipes deve ser vista com muita seriedade, pois esses profissionais devem possuir competências bem específicas que permitam boa capacidade analítica e rápida tomada de decisão em um ambiente aberto ao público e acessado por milhares de pessoas diariamente;
- 4) O investimento em treinamento deve ser massivo e constante com foco na antecipação de fatos típicos, através de análise comportamental e nas respostas, treinando, mediante a aplicação de exercícios simulados, os protocolos pós ocorrência.

Atualmente o segmento conta com legislação própria, normas, instruções e vasto conteúdo acadêmico específico para prover o gestor de riscos de informações suficientes para que não deixe seu empreendimento desguarnecido de um bom programa de gerenciamento de riscos. Não obstante, Bem antes do cenário atual, **Henry Fayol**, já defendia em seu legado literário, o importante “papel da segurança em proteger vidas e patrimônio de problemas...”.

Ainda nesta linha o engenheiro apregoava (1990, p. 65) que prever é planejar, investigar profundamente o futuro e traçar um plano de ação a médio e longo prazo a fim de preparar a empresa ante as adversidades, ou seja, mesmo se tratando do aludido modelo de administração é possível identificar compatibilidades, principalmente quando pensamos em cenários prospectivos na segurança corporativa.

Para segurança empresarial, “O objetivo de elaborar cenários, específicos para a área de riscos corporativos, é o de poder antecipar as variáveis que, por ventura, possam interferir nas metas da empresa”. (BRASILIANO, 2003 p. 47).

Para BRASILIANO (2003, p.51) a dinâmica das variáveis observadas dentro da gestão de riscos delimita a modelagem de cenários para apenas um ano.

Nesse mesmo diapasão, um dos grandes expoentes da segurança corporativa, o especialista e professor Claudio Moretti em: < <http://www.administradores.com.br/artigos/cotidiano/cenarios-em-seguranca-visao-prospectiva/106652/>>. Acesso em: 22 março 2018. expõe justa e doura crítica ao empirismo dos empresários e profissionais da área que ainda acreditam em uma implantação e gestão de segurança sem aplicação de

metodologia e respaldo científico, empregando seus recursos da mesma forma que vinte anos atrás.

É fato que tudo está em constante mudança, assim como os cenários e, se existe mudança, é salutar que hajam novos estudos, diagnósticos e análises por parte dos profissionais que cuidam destes grandes centros de entretenimento e laser, caso contrário, continuaremos a ver alguns shoppings sofrendo com ataques recorrentes e outros, cujos profissionais entenderam a necessidade de mudança, mantendo seus empreendimentos resguardados das ações criminosas.

Por isso, nosso QAP total, full time e real time nos estudos da ciência segurança.

BIBLIOGRAFIA

FAYOL, H. **Administração Industrial e Geral**: previsão, organização, comando, coordenação e controle. São Paulo: Atlas, 1990.

DAMODARAN, Aswatah, **gestão estratégica do risco**, São Paulo: Bookman, 2009

BRASILIANO, Antonio Celso Ribeiro, **gestão e análise de riscos corporativos**, São Paulo: Sicurezza, 2010

MORETTI, Claudio dos Santos, (www.administradores.com.br) Site da internet, acesso 22/03/2018. Artigo cenários em segurança: visão prospectiva.

AGRADECIMENTOS

Nelson Junior: Gerente de segurança – São Paulo

Marcelo Cabral: Gestor de Segurança – Rio de Janeiro

Tiago Miranda: Gestor de Segurança – Rio de Janeiro

Djalma Santos: Coordenador de Segurança – Rio de Janeiro

Ubiratan Gomes: Coordenador de Segurança – Rio Grande

AUTOR

André Anjos C.P.S.I / C.I.G.R / M.B.R / C.I.S.I, DIDS

Gestor de Segurança no segmento varejo;

Graduado e Pós-Graduado em Segurança Privada e Ordem Públicas;

Especialista em riscos corporativos com ênfase em grandes empreendimentos;

Especialista em Administração de Segurança;

Certificado Profissional em Seguridad Internacional-C.P.S.I.;

Certificado Internacional en Gestion de Riesgos-C.I.G.R.;

Master Business In Risk-MBR;

Certificado Internacional em Segurança Integral e Prevenção de perdas-C.I.S.I.;

Diplomado Internacional en Dirección de Seguridad – DIDS;

Sócio Honorário CEAS-INTERNACIONAL.

A COLETA DA INFORMAÇÃO NO PROCESSO DE INTELIGÊNCIA COMPETITIVA

1. CONCEITO DE INTELIGÊNCIA COMPETITIVA

A Inteligência Competitiva nas organizações de hoje, agrega valor à informação. Por esta razão, é que a Inteligência Competitiva possui uma associação explícita com os sistemas de planejamento e administração estratégica. A Inteligência Competitiva está e deve estar ligada à área estratégica das empresas e instituições porque a informação por si só é factual. É um número, estatísticas, dados recolhidos sobre pessoas, tecnologias, processos de vendas e marketing, estruturas de empresas, custos e preços, legislações governamentais, entre outras atividades que pareça interessante. As decisões não devem ser tomadas embasadas somente nestas informações. Mas sim na filtragem e análises destas informações, transformando-as em inteligência.

Segundo Larry Kahaner o conceito de IC é “A Inteligência Competitiva não é uma função, mas sim um processo. Dessa forma, ela deve aparecer na empresa, em todos os segmentos e aspectos do negócio, como uma atividade contínua e não relegada a uma área, divisão ou unidade de negócio”. Isto significa que a principal razão de uma empresa ou instituição possuir a Inteligência Competitiva é o de suportar as tomadas de decisões. As informações analisadas, transformadas em inteligência, segundo Tyson são imprescindíveis para as empresas serem capazes de tomar decisões estratégicas acertadas, não podendo ser mais suficiente uma análise anual do ambiente de negócios.

O programa de Inteligência Competitiva, em uma empresa, formalizado pode:

1. Antecipar mudanças de mercado;
2. Antecipar ações do concorrente;
3. Descobrir novos ou potenciais concorrentes;
4. Conhecer os processos críticos da concorrência;
5. Conhecer sobre novas tecnologias, produtos e processos que possam afetar o negócio da empresa;
6. Saber sobre mudanças políticas, legislativas ou regulamentares que possam afetar o negócio da empresa;
7. Introduzir novos negócios;
8. Ajudar a implementar as ferramentas de sucesso de gerenciamento na empresa.

2. CICLO DE INTELIGÊNCIA COMPETITIVA

A unidade de um sistema de Inteligência Competitiva é o ciclo da inteligência. É o processo pelo qual informações cruas são transformadas em inteligência.

Segundo Kahaner o processo, o ciclo de inteligência usado pelas empresas é o mesmo utilizado pelas agências governamentais, inclusive pela

própria CIA, que são quatro: planejamento, coleta, análise e disseminação. Utilizamos o ciclo abaixo, com cinco fases do processo, que é o controle e avaliação.

1. Identificar os fatores críticos de sucesso
2. Criar a rede de prospecção
3. Difundir a inteligência para o decisor agir
4. Transformar a informação em inteligência

Este artigo irá tratar da segunda fase do processo da Inteligência Competitiva, a Coleta das Informações. A coleta envolve obter as informações cruas que serão transformadas em Inteligência útil — alguma coisa que possa ser usada pela alta gestão. É como matéria-prima levada para uma fábrica para ser transformada em produto acabado.

Esta fase envolve a operacionalização da coleta de informações, que serão transformadas em inteligência. Os coletores de informações devem e podem usualmente encontrar qualquer informação de modo ético e legal. A coleta também envolve o processamento da informação de forma a poder ser tratada, transmitida, e armazenada eletronicamente.

Nesta fase também que a IC implanta sua rede de coletores. O grande desafio dos sistemas de Inteligência Competitiva é a construção de redes que verdadeiramente colem informações de forma sistemática e rotineira, o que não deve demandar uso intensivo de processos automatizados ou grandes estruturas organizacionais.

3. TIPOS DE INFORMAÇÕES

Há muitos tipos de informação, mas, por enquanto, vamos dividi-las em duas categorias: primárias e secundárias.

Informações primárias são fatos vindos diretamente da fonte e não adulterados. Essas fontes são fontes primárias. A fonte poderia ser um presidente, agência governamental ou qualquer um mais que tenha acesso à informação absolutamente correta. É uma informação que não pode ser mudada, alterada ou disfarçada por opiniões ou seleções (por seleção queremos dizer o que acontece na mídia. Ainda que um dado possa ser preciso, ele ainda assim foi escolhido pelo repórter, entre vários outros dados, que poderiam ser publicados).

Exemplos de fontes primárias são as comunicações em que o presidente de uma companhia dá informações sobre os planos de sua empresa, sua vida financeira, tecnologias, entre outras. Relatórios anuais e outras publicações são também considerados como fontes primárias. Relatórios de Comissões de Câmbio e de seguradoras, também.

As informações primárias devem ser consideradas absolutamente acuradas, já que as fontes também devem ser consideradas deliberadamente confiáveis. Você pode levar em conta alguns dados que foram escondidos ou mesmo erros de linguagem, mas um presidente não pode apresentar figuras erradas em apresentações e declarações, sob pena de ser crucificado, no dia seguinte, pela mídia.

Os itens que você observa por si mesmo são também fontes primárias. Se você conta o número de carros num estacionamento, no período noturno,

com a intenção de determinar o número de funcionários nesse período, este é um dado de fonte primária. O mesmo vale para coisas que você observa em uma feira e ou congresso e através de literatura. O mesmo para fotos e Vídeos. Os dados governamentais também devem ser considerados como fontes primárias. Os coletores governamentais de informações frequentemente obtêm seus dados a partir do próprio ramo industrial, usando pesquisas e questionários, o que faz essas informações serem disponíveis para todos. Os arquivos de relatórios em agências governamentais são excelentes fontes de informações primárias, assim como os relatórios de documentos da Justiça.

As fontes primárias são os grãos sagrados da informação. Obter material primário deve ser considerado como uma meta também primária Mas não é sempre possível obter isso.

A outra categoria de informações são as obtidas através de fontes secundárias. Fontes secundárias oferecem informações alteradas. As informações secundárias são mais comumente encontradas do que as informações primárias e algumas vezes é o único tipo de informação que você pode obter sobre um determinado assunto.

As informações secundárias incluem fontes como jornais, revistas, TV e rádio. Informações escritas sobre empresas em diversos veículos como, por exemplo, publicações de um congresso. Trabalhos acadêmicos assim como relatórios de analistas sobre empresas devem ser considerados como informações secundárias.

O que separa material primário de secundário é que o material primário é cru, inalterado e usualmente de forma inteira, enquanto o secundário foi selecionado, comparado com informações mais amplas (como por exemplo, com uma palestra na TV), ou alterado por opiniões (como as de um relatório de analista).

Isto não quer dizer que nas fontes secundárias tenham menos importância ou mesmo menos precisão que as primárias. Isso significa, para você, é que, quando você coleta informações, precisa dar pesos diferentes a cada uma, baseando-se em sua origem e em seu trajeto até chegar ao seu conhecimento.

Fontes secundárias podem, às vezes, serem melhores que as primárias no que concerne à qualidade da informação. Você pode frequentemente obter mais intuições sobre um determinado assunto a partir de análises de jornalistas. Essas pessoas frequentemente veem um ramo industrial como um todo e pode oferecer prismas que você não conseguiu enxergar. Elas observam tendências de que você não teve notícia e possuem fontes confidenciais no meio do ramo.

Por exemplo, o presidente de uma empresa pode falar que sua companhia pretende crescer 15% no próximo ano fiscal. As coisas parecem óbvias, mas um jornal fala que, a partir da percepção de seu repórter, que consultou analistas do ramo, os tais 15% não serão fáceis de conseguir.

O que isso pode significar para você? Muitas coisas. Primeiro, você sabe o que o tal presidente acredita e, ao mesmo tempo, sabe o que a rua pensa — são dois dados importantes e úteis de informação.

E você não terá apenas a sugestão emitida pelo presidente, mas também a opinião de um jornal, em que estão presentes os argumentos sobre o que ele disse.

Quando você coleta informações secundárias, você fica mais familiarizado com as idiossincrasias das fontes. Algumas são mais precisas do que as outras; algumas são mais completas; algumas são simples demais; algumas têm desvios e por aí adiante. Eventualmente, você percebe qual o peso que deve dar a cada fonte de acordo com a sua origem e com a pessoa que emitiu a informação.

Quando coletando informações a partir de mídias internacionais, é importante prestar atenção no que diz respeito às diferenças entre o jornalismo americano e o estrangeiro. Os jornalistas americanos tendem a ser imparciais e os europeus e latino americanos, por exemplo, os britânicos e brasileiros, jamais deixam de expressar o seu ponto de vista particular. Isto, na realidade, não é obrigatoriamente negativo. A opinião dos outros pode ser importante e a informação, mesclada dessas opiniões, podem não apenas informar como também sugerir uma linha de conduta ou mesmo de mudanças.

4. A IMPORTÂNCIA DA COLETA DE INFORMAÇÕES

Empresas com programas de Inteligência competitiva engajam-se em dois tipos de procedimento quanto à coleta de informações.

Primeiro, elas coletam as informações (tanto a resposta de um problema quanto a primeira fase de sua solução), por uma razão específica quanto em resposta a um pedido da gerência.

Segundo, elas coletam informações que estão salvas e construídas dentro de um banco de dados sobre uma empresa, um ramo, e assim por diante. Esta informação é atualizada regularmente e assim ela pode ser consultada quando necessário. De maneira ideal, ambas essas atividades ocorrem ao mesmo tempo.

5. CRIATIVIDADE NA COLETA DE INFORMAÇÕES

Num mundo perfeito e bonito, você pode receber uma pergunta da gerência e sair procurando a resposta. Em algum lugar você encontrará o que precisa, seja num artigo de jornal ou num relatório anual de empresas.

Por exemplo, suponha que você quer saber a quantas anda o plano de crescimento de seu concorrente para o próximo ano. Você olha no relatório anual e lá está a informação: o presidente anteviu o crescimento em 10% para o próximo ano.

Então, há a vida real. Frequentemente lhe são solicitadas informações que não estão prontamente disponíveis, e tentar satisfazer os requisitos das gerências transforma-se numa matéria altamente criativa.

As pessoas que são inclinadas a resolver problemas à base da força bruta não permanecem muito tempo na atividade de coleta de informações. Certamente há métodos que podem encontrar as respostas rapidamente — como no exemplo citado acima — mas encontrar outras informações requer que você tenha um amplo conhecimento do negócio, do ramo ou setor.

Pode requerer que você pense em termos de várias etapas antes de encontrar um número para análise. Podemos citar um exemplo, retirado do livro de Nolan, Confidential: “Em 1989, os gerentes da Coors estavam preocupados com os relatórios que diziam que a Anheuser-Busch estariam tentando uma grande arremetida no mercado das Montanhas Rochosas com a Budweiser e a

Bud Light. A Anheuser-Busch esteve influenciando cidades nas costas Leste e Oeste com propagandas e promoções, fazendo algumas incursões às custas da Coors. Coors é uma das mais fracas das três grandes cervejarias (Miller é a terceira). A área das Montanhas Rochosas tem sido sempre a mais forte para a Coors e perder participação de mercado em seu território seria não apenas prejudicial, mas também humilhante. A pergunta era: Teria a Anheuser-Busch capacidade de produção em sua fábrica de Denver para acompanhar a ofensiva de publicidade e promoção para fazer uma campanha eficaz do ponto de vista custo/lucro? A resposta foi elegante. Usando apenas relatórios públicos, um consultor externo de IC acessou os arquivos da Anheuser-Busch junto à Environmental Protection Agency (EPA — Agência de Proteção Ambiental), no que dizia respeito à sua descarga de águas-usadas. A partir disso ele foi capaz de determinar a capacidade máxima de produção da empresa. E soube que ela não tinha capacidade de produzir tanta cerveja quanto seria necessário para um lançamento de sucesso na área. Coors, que tinha planejado gastar milhões de dólares em contra-promoção e publicidade, foi capaz de alocar seus recursos em outra área. Todas as empresas desse ramo precisam relatar a quantidade e destino de suas águas-usadas para o EPA. Como o coletor sabia disso? É uma das coisas que uma pessoa perfeitamente integrada em seu ramo de negócios precisa saber. No mínimo é uma ferramenta que deve ser conhecida e bem explorada.” Este exemplo mostra três lados da Inteligência Competitiva:

- Informação: a quantidade de águas-usadas que era descarregada
- Análise: a partir desse dado, extrapolou-se a capacidade de produção
- Utilização da informação: Coors decidiu postergar uma possível contra-campanha.

Podemos citar outro exemplo do livro de Nolan, Confidential: “Uma empresa japonesa queria construir um processador de papel na Georgia e precisava saber a capacidade de uma fábrica próxima e quanto papel ela estava produzindo. Se a fábrica estava sendo sub utilizada, não havia sentido em construir uma outra. Por outro lado, se a fábrica estava funcionando em sua capacidade total, haveria espaço para uma outra porque havia muitas fazendas de reflorestamento na região. Um consultor externo contratou alguém para contar o número de vagões que deixavam a fábrica: todavia, não havia garantias de que todos os vagões estavam cheios. Trabalhando com um químico e um metalúrgico, o consultor foi capaz de determinar o peso que passou sobre os trilhos através da medição da quantidade de ferrugem que ali ficava após cada viagem. Por uma simples conta de subtração, ele descobriu o peso que cada vagão estava carregando. A partir desse número, ele extrapolou a quantidade de papel que estava sendo produzida. Mas isso era apenas uma parte da resposta. Estariam as máquinas da fábrica operando em plena capacidade? Em seguida, o consultor descobriu que espécie de máquinas a fábrica utilizava simplesmente perguntando para alguns trabalhadores. Assim, descobriu através deles quanto material essas máquinas eram capazes de processar. Dessa forma ele definiu que as máquinas estavam trabalhando a maior parte do tempo com 90% de sua capacidade e os japoneses decidiram que valia a pena construir outra fábrica”.

Mais uma vez, a história mostra como uma pessoa criativa encontra a resposta para uma pergunta específica.

- A informação: peso e número de vagões e quantas viagens faziam; a capacidade da fábrica de produzir papel.
- Análise: dados esses números, qual a capacidade estimada de operação da fábrica.
- Utilização da informação: havia espaço na região para mais uma fábrica.

Os dois exemplos são criativos. O primeiro caso é um que usou informações de domínio público. O segundo caso envolveu o uso de informações mais complicadas e não-públicas. Ambos os métodos realizaram o trabalho.

Assim, é preciso olhar primeiro para as informações de domínio público e onde você as pode obter.

6. INFORMAÇÕES DE DOMÍNIO PÚBLICO

Informações de domínio público é um vasto oceano de dados que são abertos e disponíveis para qualquer um que os queira pesquisar. Algumas delas são produzidas por instituições governamentais e outras pela mídia, associações e pelas próprias empresas.

Pelo fato de vivermos numa sociedade de leis e regulamentos, há uma certa quantidade de trabalhos publicados que são envolvidos no dia-a-dia dos negócios. Isto é especialmente verdade para ramos de atividades que são pesadamente regulamentados tais como comida, agroindústrias, farmacêutica, linhas aéreas e outras. A ideia dessa regulamentação é a segurança pública. Quando a segurança é um item, há uma grande quantidade de trabalhos publicados que precisam ser arquivados. Quase todos são de domínio público. Uma trilha de papéis também acompanha as empresas de capital aberto. Quando este é o caso, relatórios de seguradoras e comissões de câmbio, bem como documentos de corporações estatais estão disponíveis.

Quando olhando para empresas e para as informações que você pode obter sobre elas no domínio público, você deve primeiro buscar em três jurisdições governamentais: federal, estadual e municipal.

Federal

Empresas de capital aberto têm de arquivar uma resma de papéis junto às seguradoras e à Comissão de Câmbio. Esses papéis são cruciais para a construção do perfil de seus concorrentes.

Os documentos podem ajudá-lo a montar um quadro da situação financeira da companhia, seus planos estratégicos baseados nos comentários da gerência e planos de marketing. A verdade maior dos relatórios vem com a comparação dos atuais com os dos anos anteriores. Você pode ter uma boa ideia de para onde a empresa está olhando e como ela pode ter mudado seus focos no correr dos anos.

Estadual

No mínimo os estados requerem que as empresas — mesmo as de capital fechado — relatem a cada ano, para o governo, usualmente a secretaria de estado, se elas foram incorporadas.

Os estados variam muito com relação às informações contidas nessas repartições públicas, mas elas podem lhe fornecer alguns dados sobre seu concorrente.

Municipal

A maioria dos municípios exige que as empresas em sua jurisdição tenham licenças de operações. Estas licenças, que estão no domínio público, contam quem possui a empresa, onde ela está localizada e se é uma subsidiária ou não.

Um dos relatórios locais mais útil é a permissão de construção. Esse relatório pode lhe dizer o que o seu concorrente está planejando. Quase todos os empreiteiros acompanham de perto os planos de seus concorrentes através dos processos de permissão de construção. Isso é especialmente verdade quando um projeto necessita de uma variação de zoneamento. Essas variações exigem que o requerente dê informações detalhadas sobre plantas baixas, locações, plantas hidráulicas, elétricas e assim por diante.

A Mídia

A mídia é uma fonte secundária porque contém não apenas informações cruas, mas também, usualmente, alguma análise.

Pesquisas mostraram que no Japão as empresas usam os jornais pátrios mais do que qualquer outra fonte isolada de informações porque os jornais japoneses de negócios contêm muito mais informações profundas do que quaisquer outros em todo o mundo.

Você deveria também saber que nem todos os jornais apresentam o texto completo de uma história. Por exemplo, quando um serviço como a Associated Press ou Reuters, envia uma história, o jornal associado pode cortar parte do texto por falta de espaço. E você nunca ficará sabendo o quanto ou o quê foi cortado, a menos que você consiga ler o artigo original. Assim, se você vê um artigo no jornal que o interessa, e que foi originado por uma agência noticiosa ou mesmo um outro jornal, você deveria encontrar o original. De outra maneira, possivelmente estará faltando alguma informação crucial.

Uma das melhores coisas sobre jornais é que a maioria das histórias pode ser obtida usando bancos de dados on-line. Jornais permitem que bancos de dados possam reproduzir e distribuir histórias. Porque as histórias estão num banco de dados eletrônico, você pode encontrá-las através dos nomes das empresas, nomes dos produtos, nomes das pessoas ou qualquer outra palavra-chave ou termo que você deseje.

Este procedimento é também rápido. Você pode obter informações imediatamente, embora se deva ter cuidado por causa de alguma defasagem com relação à publicação no jornal. No caso de revistas, a defasagem pode ser maior.

Uma outra maneira de coletar artigos de jornais e de revistas é através de um serviço de clipping. Você lhes dá as palavras-chaves e o serviço vai lhe enviar os artigos de seu interesse, diariamente, semanalmente ou mensalmente, conforme o acordo. Isto não é apenas conveniente, mas frequentemente esses serviços de clipping lê em jornais, revistas e newsletters de muito pequena circulação e que não figuram em bancos de dados.

Não espere descobrir tudo o que você quer saber sobre um concorrente através de uma ou duas fontes. Seu trabalho é colher fragmentos que podem construir o total da informação.

Algumas das melhores fontes de informação são os boletins especializados. Artigos neles publicados são sempre mais focados que outros da imprensa geral e são frequentemente escritos por técnicos de empresas — suas concorrentes. Certamente, um engenheiro escrevendo num boletim especializado, não estará transmitindo nenhum segredo de marca; contudo, ele pode falar sobre algumas coisas sobre seus projetos em andamento ou sobre produtos que você ainda não sabia. Você pode encontrar uma gema ou duas. E, porque isso vem de uma pessoa intimamente ligada à empresa, a informação é precisa e confiável.

Outro aspecto de examinar a mídia é digno de mencionar. A informação para IC não é encontrada apenas nas seções de novidades e especialidades, mas também em outras partes de um jornal ou revista: os classificados e anúncios institucionais.

Varejistas têm estudado os anúncios de seus concorrentes por anos para ver que produtos eles estão trazendo à luz do mercado, assim como seus preços.

Associações de classe

As associações de classes empresariais são boas fontes de informações sobre determinados setores de um ramo, mas você não encontrará informações específicas sobre as empresas-membros. O que você vai encontrar são dados sobre o ramo, projeções, mercados e assim por diante. Obviamente, isso pode ser útil para saber sobre um ramo genericamente, especialmente sobre itens correlacionados a ele.

Porém, há um artifício que pode ajudá-lo, a saber, sobre empresas individualmente. Se a associação é dominada por várias grandes companhias, quaisquer informações sobre o ramo provavelmente refletem essas grandes empresas, desproporcionalmente.

Por exemplo, a associação queixa-se que seus membros compreendem 70% do mercado como um todo. Se você estimar que duas empresas dominam equitativamente a associação, então você pode ter uma boa estimativa de quanto uma empresa participa do mercado como um todo. Neste caso, é provável que esse valor seja de 35%.

Bancos de dados

Bancos de dados são excelentes ferramentas para estabelecer uma rede de peso para iniciar suas pesquisas de informações. Você pode acessar diretamente os bancos de dados ou ter uma empresa que o faça baseada em

suas palavras- chaves. Podemos dividir os bancos de dados em duas categorias:

- Os que contêm artigos
- Os que contêm números

A primeira categoria contém artigos de jornais, revistas, transcrições de trabalhos em TV e rádio, newsletters, press releases, relatórios governamentais. São usualmente fontes secundárias, embora também as haja primárias.

Os bancos de dados com números apresentam patentes, informações financeiras, propaganda, informações sobre câmbio, dados sobre export/import, vendas, estatísticas. São dados crus, não-filtrados. São principalmente fontes primárias embora também as haja secundárias.

Esta lista é apenas uma fração mínima do que está disponível on-line. Muitas empresas de serviços oferecem populares bancos de dados para seus clientes, assim você não precisa subscrever cada um individualmente. Porém, aqueles bancos de dados mais obscuros e esotéricos têm de ser lidados diretamente com o compilador.

Também, muitos desses bancos de dados são agora oferecidos em CD. Embora eles possam não conter informações super atualizadas, eles são fáceis de pesquisar e podem ajudá-lo a ter uma perspectiva histórica de seus concorrentes e do ambiente competitivo.

Internet

Nenhum legítimo livro de negócios pode ser publicado hoje em dia sem mencionar a Internet. Bastante simples, a Internet é uma rede que conecta computadores por todo o mundo. Assim, o que nós temos? Nós temos milhões de pessoas entrando na Internet através de colégios, universidades, hospitais, agências do governo. Poucos anos atrás particulares e empresas tinham acesso à Internet através de Ips comerciais. A Internet alcança virtualmente todos os países do mundo.

Uma vez que você está na Internet, você pode usá-la para e-mail e troca de mensagens com qualquer um mais na grande rede, ou você pode usá-la para outros serviços de informações.

Quase todos os colégios, universidades e institutos de pesquisa, no mundo inteiro estão na Net. Todas são acessíveis por qualquer um na Net. Esses bancos de dados governamentais são excelentes fontes de informações para uso em Inteligência competitiva.

Estar a par das regulamentações governamentais é um de seus imperativos em IC. Você pode obter textos integrais de regulamentos, bem como de exigências de procedimentos, usando a Internet.

Todavia, a Internet ainda é muito uma instituição não-comercial. Uma das razões dessa mudança são as chamadas web pages e a configuração www (world wide web). A web é a única configuração de tudo que está na rede e fez usuários- amigos com funções de hipertexto. Hipertexto é um sistema em que você lê o texto e quando chega a uma palavra ou frase em negrito ou numa cor diferente, você clica o mouse (ou aperta enter) no seu computador e

isso faz um link com a informação sobre o assunto em outra parte da Net. Esses links de hipertexto usam essas páginas como base.

Algumas webpages também contêm mecanismos de busca. São programas utilizados na web que permitem procurar por informações através de palavras-chaves ou frases.

Embora nenhum mecanismo de busca seja absolutamente completo, eles podem pesquisar vastas áreas na Internet. Considerando-se a quantidade de informações presente na Internet, essas buscas podem ser incrivelmente compreensíveis. Na essência, usando vários desses mecanismos de busca, você pode encontrar todas as informações disponíveis na Internet sobre qualquer assunto.

Muitas empresas estão montando web pages e elas contêm propaganda e informações sobre seus serviços. Muitas consultorias de IC possuem web pages. O poder da Net não está apenas em quanta informação disponibiliza, mas também em quantas pessoas alcança. A confiança na Net também é imensa.

Se você faz uma pergunta no lugar certo, você pode encontrar exatamente a resposta que está procurando.

Também existem grupos muito específicos que automaticamente o porão em seu mailing list. Para assinar, envie um e-mail para o servidor da lista com as palavras requeridas no corpo do texto. A lista é automaticamente manipulada por um computador.

É seguro dizer que há mais informações cruas eletronicamente contidas na Internet do que em qualquer outra entidade do planeta. E também, igual quantidade de Inteligência.

7. INFORMAÇÕES FORA DE DOMÍNIO PÚBLICO

O fato de uma informação não estar acessível em domínio público não quer dizer que ela seja privada ou confidencial. Simplesmente quer dizer que você precisa ser um pouco mais persistente e hábil para encontrá-la.

Momento de mudança

Leonard Fuld, da Fuld&Company, surgiu com esse conceito único que ele chama de momento de mudança. É durante tempos de mudanças massivas que acontece crescente atenção a certas empresas. Durante esses tempos a mídia produz cargas de artigos, uma grande quantidade de trabalhos publicados pode ser encontrada e muitos documentos de domínio público são produzidos.

Inteligência humana

Agências de Inteligência governamentais gostam de chamá-la de humint, e isso significa Inteligência humana ou, pondo em outras palavras, o que alguém conta para você.

Quando alguém de sua força de vendas lhe fala sobre um cliente cuja empresa pode estar para vender, isso é humint. Quando você escuta um rumor em seu clube de que um novo gerente está chegando para um de seus concorrentes, isso é humint. Quando você envia um de seus funcionários para a inauguração de uma nova fábrica de seu concorrente e ele toma notas de tudo o que viu, isso é humint.

Apenas pergunte

Uma das maneiras mais diretas de encontrar informações sobre concorrentes, é perguntar. Clientes normalmente dividem com você suas opiniões sobre os serviços, produtos e preços de seus concorrentes, se você lhes perguntar. O cliente estará disposto a lhe contar porque isso atende seus propósitos de obter o melhor produto pelo melhor preço. Porém, tenha em mente que seu concorrente pode estar fazendo a mesma coisa: perguntando o mesmo para o seu cliente, sobre você.

As pesquisas de clientes são uma das ferramentas mais usadas. Essas pesquisas, que são feitas sobre os seus clientes, vão ajudá-lo a comparar sua empresa ou você mesmo com o concorrente, a partir da perspectiva dos clientes.

Essas pesquisas podem ser feitas por escrito ou por telefone e, nesses casos, o resultado é sempre pequeno porque você não se identifica e não conta para as pessoas a razão de suas perguntas.

Não há nada ilegal ou antiético perguntar para seu concorrente como andam suas vendas, pedir-lhe brochuras sobre taxas e catálogos de produtos. Também não há nada errado em perguntar ao pessoal de vendas de seu concorrente sobre o tamanho de seu departamento, quanto tempo demora a entrega dos produtos e que espécie de documentação de vendas eles carregam. São perguntas que um cliente normal pode fazer, assim a empresa não pode manter essas informações no campo da confidencialidade.

Muitas empresas inscrevem-se em mailing lists para receber brochuras de vendas ou malas-diretas de ofertas, para monitorar seus concorrentes. Esta atitude apresenta benefícios por dois lados: você não apenas pode estar atualizado sobre os produtos de seu concorrente, como também pode avaliar quanto ele está gastando em mala-direta e propaganda, o que é uma outra peça importante do quebra-cabeça da Inteligência.

No Japão, agentes de companhias falam entre si sabendo que quando a informação roda, todos se beneficiam. Mesmo não esperando descobrir grandes segredos de marca, as pessoas que confiam numa outra — especialmente aquelas que trabalharam juntas em outras épocas — frequentemente conversam sobre suas empresas. A chave é enfatizar o registro dessas informações. E lembrar que tanto se recebe quanto se dá.

Através desses encontros você pode ser capaz de montar uma rede de empresas como a sua e que não cometem entre si por causa de considerações geográficas. Isto é muito comum com freelancers e aqueles com um pequeno serviço independente ou empresas varejistas. Você pode livremente partilhar informações com esses do mesmo ramo que o seu sem se preocupar em estar fornecendo seus segredos para um concorrente que seja seu vizinho.

Pessoal de vendas

De longe, a melhor fonte de Inteligência humana vem de seu pessoal de vendas. Eles estão do lado de fora, na linha de frente, aprendendo sobre seus concorrentes e tentando superá-los em vendas.

De fato, o pessoal de vendas instintivamente coleta informações que lhe podem trazer benefícios, mas a maioria dos vendedores guarda-as para si ou as divide apenas com os colegas ou seu gerente direto.

A informação não parece chegar à gerência superior.

Uma das razões é que os vendedores já têm muito trabalho em papel para adicionar mais um, que eles consideram de baixa prioridade. Um caminho para contra-atacar essa mentalidade é tornar mais fácil partilhar coisas que eles tenham percebido. Algumas companhias possuem um número 0800 ou possibilitam notas rápidas que podem ser enviadas por fax ou encaminhadas com simplicidade. Um e-mail também funciona bem. Não há nada errado num sistema de baixa tecnologia para coletar informações vindas do pessoal de vendas ou de qualquer outra pessoa.

Um outro caminho seguro para seduzir à participação é assegurar que qualquer informação que funcione para cima, também funciona para baixo. Em outras palavras, o pessoal de vendas poderá se beneficiar dos resultados das informações que eles fornecem à unidade de CI ou ao seu gerente.

Observação

Há uma tendência de se achar que IC é totalmente intelectual. Ou seja, algumas pessoas gostariam de sentar em seus escritórios, entrar num banco de dados, ler o jornal ou falar ao telefone e, através disso, conseguir tudo o que precisam.

Ainda que essa tática em forma de torre de marfim funcione para muitas situações, não a verdade absoluta. Algumas vezes você tem de sair do escritório e ver o que está acontecendo. Mais uma vez, eis porque o pessoal de vendas é uma fonte de informação tão valiosa.

Um supervisor de logística de uma grande empresa brasileira diz que, uma vez por mês, ele fica observando, de algum local público, com um bloco de notas na mão, o sistema de logística de seu concorrente. “Eu vejo quantas pessoas eles têm para o trabalho, quantas embalagens carregam, quantas há no container, e coisas assim. Isso me dá uma boa ideia de como comparar com o meu pessoal.”

O supervisor disse que ele está particularmente interessado em ver como eles carregam os caminhões sob tempo ruim. Parte da plataforma está exposta ao tempo e o trabalho vai mais devagar, pois os carregadores têm de tomar cuidado para não escorregar. Observei que a velocidade de carregamento cai em cerca de 15% durante a chuva. Algumas vezes cheguei a ficar tentado a lhes dizer que o custo/benefício da compra de uma cobertura que protegesse a plataforma da chuva seria conveniente. Mas isso é um dado que obtive e não estou disposto a partilhá-lo com o concorrente.

Enquanto observações usando baixa tecnologia, como essa, são frequentemente eficientes, estamos vendo, dia após dia, as observações que se utilizam de alta tecnologia, se tornarem mais frequentes e mais integradas aos programas de IC.

Observação aérea

Um exemplo interessante também retirado do livro de Nolan, Confidential: “No final dos anos 70, a fábrica da Dow Chemical Company em Midland, Michigan, possuía um sistema de segurança de US\$3 milhões, uma cerca de quase 2 metros de altura, uma força de segurança de 25 pessoas e

um sofisticado sistema de alarme projetado para manter fora os intrusos. A Agência de Proteção Ambiental (Environmental Protection Agency — EPA) visitou a fábrica em 1977 para investigar alegações de emissão de gases. Uma segunda visita foi requisitada, mas desta vez a empresa impediu. A EPA pensou em conseguir um mandato judicial, mas decidiu de uma outra maneira. A EPA sobrevoou a fábrica e tirou fotografias. Sua alegação era de que a empresa não era dona do céu sobre sua fábrica e, portanto, não poderia acusar o governo de invasão de privacidade. De mais a mais, eles argumentaram que a fábrica poderia ser observada de aviões comerciais numa rota próxima. Dow discordou e ambas as partes foram para a Justiça. Em novembro de 1984, a Corte de Apelação foi favorável à Dow. Essa decisão levou a recurso junto à Corte Suprema (havia um caso similar envolvendo um plantador de marijuana que se queixou que os aviões das forças legais estavam invadindo a sua privacidade; ele perdeu) e esses casos acabaram por determinar o estágio de legalidade de sobre voo sobre fábricas.”

Aqui no Brasil não existe legislação específica para isso, portanto você pode, se você quiser, alugar um avião, voar sobre uma fábrica e tirar fotografias da área.

O que você pode perceber através dessas fotos?

No caso de empresas químicas ou fábricas de processamento em que os produtos se movem através das mesmas por encanamentos, por exemplo, você pode ver o fluxo do trabalho. Você poderá ver o tipo de processamento que está acontecendo, baseado na configuração. Você pode estimar as medidas dos canos e o tamanho dos tanques de estocagem. Isso pode ajudá-lo a determinar as quantidades de entrada e saída da fábrica. Satélites militares são capazes de resoluções de um metro. Estas resoluções excelentes são consideradas como informações classificadas, pois potências não- amigas podem comprar essas imagens e usá-las contra nós.

Feiras e Congressos

A face das feiras e congressos mudou na década passada. Não são mais simplesmente locais de diversão, encontros de colegas, ou de tentar fazer vendas. Congressos e feiras transformaram-se numa das principais oportunidades de atividades de IC.

Congressos e feiras são únicos no que diz respeito a um lugar onde se pode abrir conversações com concorrentes. Em soma, ainda que muitas companhias tentam esconder e complicar as informações sobre seus produtos, elas trazem essas informações claramente para os congressos e feiras. As empresas japonesas são artistas na Inteligência em feiras e congressos. Seu pessoal mergulha, pegam o que podem em termos de material impresso e aprendem tudo o que conseguem das exposições.

Para conseguir as mais completas vantagens de Inteligência em congressos e feiras, você precisa planejar antes. Você precisa decidir quantas pessoas enviar e que áreas você quer cobrir. Como em qualquer corrida de IC, você precisa começar com algumas questões específicas sobre seus concorrentes ou sobre o ramo em geral. Muitas empresas enviam várias espécies de pessoas para os congressos e feiras, desde pessoal de marketing

até engenheiros, passando por vendedores. Cada um deverá focar em sua área de expertise e colher informações pertinentes.

O planejamento prévio ajuda-o a identificar os estandes ou exposições para visitar e também quais palestras ou seminários esperar.

Durante a feira e congressos as equipes precisam se encontrar regularmente e discutir sobre o que aprenderam, assim como avaliar mudanças de foco com base em novas informações. Ou continuar a cobertura sem alterações até o final dos eventos. Esses encontros regulares também permitem ao pessoal ler o material que receberam e trocar ideias no sentido de avaliarem a necessidade de outras perguntas a serem feitas para o pessoal dos estandes.

Não é preciso dizer que todos das equipes devem coletar todo o material que puderem, papers, brochuras, mapas, propagandas, etc., para posteriormente usá-lo como referencial.

Uma vez num estande de um concorrente, todos devem saber quem você é e que companhia representa. É absolutamente ético você usar um crachá claro e explicativo. Isto não o atrapalhará quando entabular uma conversa com um concorrente. O que também não o impedirá de lhe perguntar sobre sua empresa e suas ofertas.

Da mesma maneira é ético você observar as pessoas que frequentam o estande, quem são e que empresas representam, bem como o tipo de perguntas que fazem. Você pode aprender bastante ouvindo o que os compradores potenciais têm para perguntar ao seu concorrente. E também é importante saber quem o seu concorrente carrega para uma área mais privativa para conversas sérias.

Presumivelmente (mas nem sempre), seus concorrentes estarão visitando seu estande e perguntando as mesmas coisas a você. Tudo faz parte do jogo. Seu objetivo é tentar conduzir as atividades de sua unidade de IC melhor do que eles.

8. ORGANIZANDO A INFORMAÇÃO DA COLETA

Alguns profissionais de IC pensam que uma empresa precisa de um sistema sofisticado para organizar, armazenar e disseminar dados. Isto não é verdade. Na maioria dos casos, o mais simples é o melhor.

Algumas pequenas empresas confiam em arquivos com informações e de fácil acesso. Esses arquivos contêm relatórios anuais, mapas de preços de concorrentes, recortes de jornais e assim por diante.

Quais as pessoas que devem ter acesso a essas informações? Qualquer um que precise.

A informação, para que o sistema funcione, precisa ser compartilhada. Se o pessoal de vendas é encorajado para conseguir informações e partilhá-las com a unidade de IC, então ele precisa ter acesso a essas informações cruas e a qualquer outra que levem para a unidade.

A única questão é como.

Para pequenas empresas com uma única locação, arquivos centralizados numa sala podem funcionar. Qualquer um pode chegar, ler o que

interessa, tomar notas e fazer cópias. Qualquer análise que queiram fazer deve ser encorajada pela unidade de IC.

Para empresas maiores, com várias localidades ou áreas de trabalho mais extensas, as informações precisam ser acessíveis através de uma central para qualquer um que delas precise.

A regra de ouro: As informações coletadas pela unidade de IC — seja pelo pessoal de IC ou por qualquer outra pessoa da empresa — precisa estar disponível para qualquer um que tenha necessidade.

A informação é claro, é analisada pela unidade de IC para a gerência, mas qualquer um que precise dela para um planejamento tático, tomar uma simples decisão ou apenas por estar querendo saber mais sobre o assunto, precisa ter acesso a ela,

Um artifício interessante é fazer a informação ser cadastrada cada vez que ela é acessada. Isso serve para dois propósitos. Primeiro, diz ao pessoal de pesquisa que tipo de informação é solicitada, quanto o é e quanto é utilizada. Segundo, dá à pessoa que contribuiu com a informação, algum tipo de retorno pelo fato de essa pessoa sentir que a sua informação está sendo útil.

E todo o material de informação, incluindo mapas, gráficos, material escrito e imagens, é colocado num arquivo que pode então ser acionado pelo usuário. Os usuários podem ter a opção de procurar o que querem por meio de palavras-chaves e frases, exatamente como fazem nos bancos de dados de jornais ou revistas.

9. CONCLUSÃO

Por tudo que foi explanado neste artigo, parece ser fora de dúvida que a coleta das informações é um dos grandes pilares do ciclo de Inteligência Competitiva.

É uma tarefa ainda executada no Brasil sem um profissionalismo, pois as empresas ainda acham que o trabalho de Inteligência Competitiva é só intelectual, é só trabalhar dentro da “torre de marfim”. Ressaltamos aqui a inteligência humana, ou seja, a forma que temos de perguntar e observar.

Portanto, o preparo cada vez mais ampliado dos profissionais dessa área deve ser um objetivo a se sempre perseguido, pois quando a coleta é feita sem eficácia, todos são atingidos, inclusive os lucros e o emprego.

Também é imperioso que os cursos de Inteligência Competitiva passem a encarar essa nova realidade, treinando as equipes de forma enfática. Assim, o ciclo de IC estará protegido de interrupção.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.

abrasiliano@brasiliano.com.br

VIOLÊNCIA URBANA E A IMPORTÂNCIA DA SEGURANÇA PRIVADA

A violência urbana e a insegurança no mundo inteiro e especialmente no Brasil é um fenômeno que se agrava de forma crescente e sem o controle eficiente por parte dos órgãos de segurança pública, a sensação de insegurança se instalou de forma permanente entre as populações em geral independentemente de classe social, se pessoas físicas ou jurídicas. Estes altos índices de violência vêm se agravando e aumentando conforme mostra as pesquisas realizadas anualmente pelo Fórum Brasileiro de Segurança Pública (FBSP) e pelo o Instituto de Pesquisa Econômica Aplicada (Ipea). Segundo o próprio FBSP (2017), mais de 63 mil pessoas foram mortas de forma violenta no Brasil.

Em 2018, já aconteceram milhares de mortes violentas de civis, além de vários policiais. Os dois últimos casos mais relevantes ocorridos no cenário de violência e intolerância atual no Brasil, foram a morte da Vereadora Carioca Mariele Franco no dia 14 de março juntamente com seu Motorista Anderson Pedro Gomes no Rio de Janeiro – RJ, e o atentado contra o então presidenciável Jair Bolsonaro ocorrido no dia 07 de setembro em Juiz de Fora - MG.

Com esse cenário de insegurança acima citado, a segurança privada passa a ter uma importância muito maior sendo cada vez mais necessária e indispensável para a segurança patrimonial e de pessoal de empreendimentos sejam eles industrial; comercial; bancário; de tecnologia; residencial; refinarias; mineradoras; etc. e por tanto, deve ser realizada com estratégias, inteligência, serviços e sistemas integrados com meios humanos, dispositivos eletrônicos, políticas, normas e procedimentos formando um conjunto de medidas e ações preventivas e de controles que são capazes de gerar uma conjuntura, na qual os objetivos e os pontos vitais desses empreendimentos estejam em condições menos expostas e mais protegidas proporcionando menor probabilidade de influências e de ações inopinadas advindas de ameaças internas ou externas. Com esse cenário, as empresas especializadas na prestação de serviços de segurança privada têm um papel fundamental e podem contribuir de forma relevante quando contratadas para tais serviços, inclusive, sendo um complemento a segurança pública conforme já estabelecido na política de segurança privada (Portaria 3.233/2012 – DG/DPF).

Como profissional de segurança empresarial com mais de 28 anos em empresas nacionais e multinacionais, alerto que devemos atentar para o fato de que para superar as dificuldades e os obstáculos que venham a surgir no mercado de trabalho, exige do profissional contemporâneo: autoconhecimento, habilidades e atitudes, além de iniciativa, criatividade, aprendizagem contínua, boa comunicação, agilidade e flexibilidade para lidar com pessoas, saber trabalhar em equipe e saber empregar os meios tecnológicos.

A América latina tem o maior contingente de profissionais de segurança privada do mundo. De acordo com um Relatório de Armas Leves publicado no ano de 2011 pelo Instituto de Estudos Internacionais e de Desenvolvimento, mostrou o quanto a segurança privada cresceu nos últimos 20 anos e empregava só naquele ano 20 milhões em média de pessoas no setor sendo quase o dobro do efetivo de policiais em atividade.

Em vários países existem leis aprovadas que buscam gerar níveis de regulamentação do negócio da segurança privada, mas é percebido também que ainda há uma carência de estruturas para realizar as atividades e ferramentas definidas por lei. Vimos então a necessidade de que cada país tenha sua legislação de segurança privada específica haja visto que atua no seguimento de segurança com a utilização de material bélico, o que carece de regulamentação, fiscalização e o controle por órgãos oficiais dos governos.

Na minha opinião, o Brasil tem uma das legislações de segurança privada mais bem elaboradas do mundo (Lei 7 102/1983, regulamentada pelo Decreto 89.056/1983 e normatizada atualmente pela portaria nº 3.233/2012 - DG/DPF, de 10 de dezembro de 2012.), faltando apenas maior empenho da CGCSP – Coordenação-Geral de Controle de Serviços e Produtos, para a fiscalização e o combate aos que praticam esta atividade de forma ilegal, tidos como clandestinos.

As empresas especializadas na prestação de serviços de segurança privada no Brasil, contam com o apoio institucional e na interação com os órgãos governamentais e entidades de classe através da Federação Nacional das Empresas de Segurança e Transporte de Valores – FENAVIST, em São Paulo existe o SESVESP e nos demais estados existem os SINDESP - Sindicato das Empresas de Segurança Privada.

Dr. ANTÔNIO ALVES MOTA - Estratégias; Doctor Of Philosophy In International Security Sciences, Ph.D. pela Cambridge International University, Pedagogo, Pós-Graduado em Políticas e Extensão Universitária: Análise de riscos estratégicos, Segurança Empresarial, Alta Gerência do Sistema de Segurança Empresarial, Planejamento Estratégico e Administração de Pessoal; Certificações: CPSI – Certificado Profissional em Seguridad Internacional, DIDS - Diplomado Internacional em Direccion de Seguridad e Master Superior em Direccion Internacional de Seguridad pela CEAS Internacional - Corporación Euro-Americana de Seguridad; Cursos no Brasil e no exterior sobre gestão de segurança e crise, negociação, respostas em emergência e operações antiterror. Diretor de Projetos e Relações Internacionais CEAS-BRASIL e Sócio Honorário CEAS-INTERNACIONAL.

SEGURANÇA ELETRÔNICA NO CONTEXTO DA SEGURANÇA PATRIMONIAL

Embora a economia não tenha alcançado o desejado por todos, o mercado da segurança eletrônica tem crescido anualmente, e foi neste sentido que a presidente da Associação Brasileira de Segurança Eletrônica – Abese, Selma Migliori declarou que a estimativa de crescimento para 2018 é de 8%, demonstrando que o mercado de segurança eletrônica tem um amplo mercado a ser explorado.

Mas será que a segurança eletrônica compete com o mercado de vigilância, tornando uma ameaça aos vigilantes bem como o setor de vigilância privada?

Primeiramente precisamos alinhar os conceitos para evitarmos mal-entendidos. Segurança Patrimonial é o ato de gerir o patrimônio de uma empresa, evitando perdas, enquanto que Vigilância Patrimonial, é a atividade exercida por profissionais, neste caso os vigilantes, com a finalidade de garantir a incolumidade física das pessoas e a integridade do patrimônio.

Assim sendo, há basicamente cinco grupos de mitigadores de riscos utilizados na Gestão da Segurança Patrimonial, analisando pela matriz SWOT, vamos ter quatro deles dentro do grupo fraquezas, que são os controles, infraestrutura, tecnologia ou segurança eletrônica, e pessoal, e um no grupo ameaças, que são os fatores externos. Para assegurar a segurança contra as ameaças externas, como a criminalidade, a Gestão de Segurança Patrimonial necessita mitigadores, como a infraestrutura, a tecnologia ou segurança eletrônica, os controles, e o pessoal, que dentre eles estão os vigilantes. São eles quem utilizam a tecnologia ou segurança eletrônica, bem como os demais mitigadores. Eis a importância deles se manterem atualizados com a tecnologia. Na era de tecnologia, o conhecimento e sua utilização é o fator predominante para um bom profissional.

Vimos que a segurança eletrônica não compete com a vigilância, bem pelo contrário, ela é uma forte aliada para mitigar riscos, não é por menos que as empresas estão utilizando a tecnologia a seu favor, por meio dela diminuimos as perdas, melhoramos o desempenho, diminuimos os riscos da vida dos vigilantes e otimizamos os custos.

É o exemplo da alta tecnologia como os drones, que podem ser utilizados para visualização ou rondas em locais de risco, ou de difícil acesso, assegurando uma ampla e rápida visualização, permitindo mais agilidade e assertividade nas tomadas de decisões, sem a exposição do vigilante ao risco.

Outro exemplo, é o emprego dos softwares inteligentes para identificação de suspeitos e ou atitudes suspeitas. Com sua utilização, não se limita mais na visualização de um único do monitor de vídeos de cada vez, pois o software pode analisar um número incontável de imagens simultaneamente, alertando o monitor de vídeos apenas as inconsistências identificadas, permitindo a atuação do profissional somente quando ocorrer um evento, e com isso, diminui o estresse e a fadiga deste profissional.

As identificações pelo uso de biometrias, principalmente pelas digitais e faciais, têm otimizado o controle dos acessos em locais onde há a necessidade

de controles. A rapidez no cadastramento e liberação dos usuários, nos controles dos permissionamento, bem como os registros dos acessos para consultas se tornou indispensável sua utilização.

Os sistemas de alarmes contra roubo estão cada vez mais inteligentes, e a tecnologia empregada na fabricação dos sensores tem diminuindo muito os alarmes falsos. Na maioria das vezes que ocorre um falso alarme, o principal motivo tem sido a má utilização pelo usuário, ou as especificações técnicas recomendados pelo fabricante não tenha sido observado, e não por falha da tecnologia. As empresas de monitoramento de alarmes trabalham para a satisfação dos consumidores, elas conhecem e seguem o Código de Defesa do Consumidor – Lei 8.078/90, fornecendo as melhores soluções nos projetos.

Os aplicativos – APP nos smartphones também estão sendo fortes aliados na segurança, como por exemplo o aplicativo de rondas que permite saber em tempo real a rota e o tempo das rondas, permitindo identificar os cancelamentos e ou atrasos nas rondas. Além disso, eles fornecem um checklist do que o vigilante deve verificar em cada ponto de ronda permitindo registrar as ocorrências e enviar automaticamente a informação aos gestores. Outro ponto importante, é que os APP alertam instantaneamente quando uma ronda foi realizada muito rápida (os APP permitem o planejamento de tempo das rondas), o que pode demonstrar que não foi observado com a devida atenção aos fatores de riscos e ou riscos. Geram gráficos comparativos de tempo previstos versus realizado, bem como quem realizou, o dia e horário, entre tantas outras informações úteis para uma boa gestão.

Não restam dúvidas do quanto a tecnologia tem otimizado a Gestão da Segurança Patrimonial, trazendo mais eficiência e eficácia nos resultados, diminuindo os riscos que é o objetivo principal, bem como a diminuição dos custos.

Carlos Köhler, Pós-Graduado em Segurança Privada, Graduado em Segurança Pública, MBS, CPSI, CISI, CRA, autor do livro Gestão da Segurança Patrimonial: aplicação do método PDCA, delegado CEAS-BRASIL, Sócio Honorário CEAS-INTERNACIONAL e CEO do Grupo CINDAPA.
carlos@cindapa.com.br

CEAS

JUSTIFICATIVA DO ISPS CODE NO BRASIL E PAÍSES SIGNATÁRIOS DA ORGANIZAÇÃO MARÍTIMA INTERNACIONAL

Os eventos terroristas de 11 de setembro de 2001, ocorridos nos Estados Unidos da América, motivaram uma forte preocupação na segurança marítima internacional. “Medidas especiais para aumentar a segurança marítima”, incluindo-se outros requisitos de segurança para navios, bem como requisitos para empresas de navegação e instalações portuárias. Tais medidas foram agrupadas através de um código, denominado “Código Internacional para Proteção de Navios e Instalações Portuárias” – “International Ship and Port Security – ISPS Code”, cuja finalidade é de intensificar a proteção marítima para os navios, empresas de navegação e instalações portuárias. Estes novos requisitos formam a estrutura internacional por intermédio dos quais navios e instalações portuárias podem cooperar para detectar e dissuadir atos que ameacem a segurança no setor de transporte marítimo.

A referida exigência internacional passou a integrar a responsabilidade dos governos contratantes da Convenção Internacional para a Salvaguarda da Vida Humana no Mar, de 1974 – “SAFETY OF LIFE AT SEA – SOLAS”, no tocante à adequação e adoção de medidas especiais e indelegáveis de segurança e proteção marítimo-portuária. Inclui-se como governo contratante o Brasil (signatário da IMO – Organização Marítima Internacional).

Depreende-se dos atos supracitados que coube à Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis – CONPORTOS/SENASP/MJ, como autoridade designada pelo governo federal, a atribuição de implementação do Código ISPS nos portos brasileiros, bem como a de adotar as abordagens, compromissos e recomendações da Organização Marítima Internacional (IMO), em face das diretrizes estabelecidas pela Comissão Coordenadora dos Assuntos da IMO no BRASIL (CCA-IMO) e desencadear propostas de normas e implementação de atos no campo da segurança pública portuária.

Vê-se, assim, que as ações tomadas por parte dos países membros da convenção, cujos ditames terão reflexos tanto na segurança como nos mercados internacionais. Entende-se que, para o seu pronto atendimento, há de se criarem mecanismos capazes e dotados com metas e ações que tenham por foco aperfeiçoar o Sistema de Segurança Público Portuário Brasileiro, por meio de propostas que integrem políticas sociais e ações conjuntas desencadeadas pelo poder público e pela iniciativa privada. Dessa forma, reprimam e previnam ilícitos nos portos, terminais e vias navegáveis no sentido de reduzir a impunidade, aumentando a segurança e a tranquilidade dos que utilizam instalações e embarcações no território nacional com destino à Europa e estados Unidos da América.

A não adoção de tais Normas (ISPS Code e Legislações Afins no âmbito portuário nacional e internacional) implicam na impossibilidade do nosso país não importar e exportar cargas, mediante portos brasileiros e terminais marítimos para os EUA e Europa, a contar de 01 de julho de 2004.

Cleano Lima Alves, CPSI-CIRG-CIPP-CISI-DIDS - Especialista em Segurança Privada, Doctorando em Ciencias de la Seguridad - CEAS Internacional, Diretor da Ampla Consult - Consultoria e Assessoria em Segurança, Técnico Credenciado em Segurança Portuária pela CONPORTOS/DPF/MJ, Delegado do CEAS, Capítulo PE.

UM RAIO X DA SEGURANÇA PRIVADA NO BRASIL

A 'velha' segurança patrimonial evoluiu bastante desde sua concepção, através do Decreto Lei nº 1034/69. Hoje terminologias como Segurança corporativa, compliance, governança corporativa, business impact analysis, business continuity plan, etc. são aplicadas a segurança há alguns anos, mas nem sempre foi assim. Essa importante data tem relação direta com um momento delicado da segurança pública no Brasil, pois nos idos do Governo Militar, grupos armados iniciaram ações contra as instituições bancárias com objetivo de angariar fundos para patrocinar atos de coligações de oposição. Sobre este primeiro momento da segurança privada e do ato administrativo na forma do Decreto 1034/69 cabem aqui algumas considerações, a saber:

- I. A evidente impotência do Estado (Governo Militar) diante da necessidade de responder aos fatos ora impetrados por grupos de oposição que orquestravam ações planejadas e recorrentes contra as instituições bancárias;
- II. A pouca observância do caráter qualitativo necessário para a criação de um serviço de segurança, ainda que privado, condizente com todo o cenário imposto naquela época; e
- III. A falta de diretrizes para o treinamento a ser ministrado pelas polícias estaduais, ainda sem uma padronização definida baseada nos tipos de ameaças inerentes.

Assim, com o objetivo de atender a uma importante demanda, surgiu no país a segurança patrimonial. Enquanto a atividade crescia exponencialmente em todo o Brasil, ampliando o leque de atividades além das fronteiras da segurança em instituições financeiras, percebeu-se a carência de uma regulamentação mais apropriada e esta demanda só foi atendida alguns anos depois pela ainda pouco efetiva Lei 7 102/1983, regulamentada pelo Decreto 89.056/1983 e normatizada pela portaria nº 3 233/2012 - DG/DPF, de 10 de dezembro de 2012. Esta nova Lei de 1983 revogou os arcaicos e limitados Decretos 1.034/69 e 1.103/70, porém ainda considerada frágil, serviu para regulamentar a atuação das empresas de maneira mais ampla, bem como a sua atuação operacional e administrativa no âmbito dos contratantes. A fiscalização da Polícia Federal passou a ser mais efetiva.

Recentemente um novo Estatuto foi apresentado. Trata-se do Projeto de Lei 4.238/12 que está tramitando pelas casas da "política" brasileira há mais de cinco anos e, assim como outros projetos apresentados, passando pelo crivo de comissões temáticas internas das casas até chegar para a sanção do Presidente da República. A pequena descrição feita considerando a linha do tempo parece tornar o processo simples, mas não é, pois existem inúmeros fatores e critérios avaliados pelas comissões até que um projeto se transforme de fato em uma Lei. Considerando o texto proposto no PL fica a impressão que um segmento tão importante e que cresce a cada dia merecia contar com uma regulamentação menos rasa como a que foi apresentada, mas não se pode criticar o conteúdo levado para aprovação, pois entendendo bem os meandros da nossa atual política, sua proposição tenderá a impulsionar a melhoria da categoria. Que seja bem-vinda a nova Legislação.

O crescimento do mercado privado alavancou o segmento e a criação de outros braços da segurança, como exemplo a área patrimonial e pessoal e, posteriormente, a segurança portuária, segurança condominial, segurança em shoppings e tantas outras que surgiram em razão das novas demandas oferecidas pelo amplo mercado brasileiro. A pesquisa disponível em: <<https://agenda2020.com.br/2018/01/estatuto-da-seguranca-privada-formacao-universitaria-sera-uma-exigencia-para-gestores/>> Acesso em: 10/02/2019 contém informações importantes extraídas do ESSEG – Estudo do Setor de Segurança – da Federação Nacional das Empresas de Segurança e Transporte de Valores – FENAVIST – informa que mais de 600 mil agentes de segurança privada são hoje responsáveis pela execução dos serviços de proteção do patrimônio físico das diferentes instalações empresariais em diversos pontos do país, em residências e condomínios, no transporte de cargas e suas modalidades, proteção de pessoas e seus familiares e, mais recentemente, cuidando dos grandes eventos Brasil afora. Estas são razões suficientes para receber um novo tratamento legislativo, mais do que isso, o reconhecimento das autoridades e da sociedade.

Dados de evolução das empresas



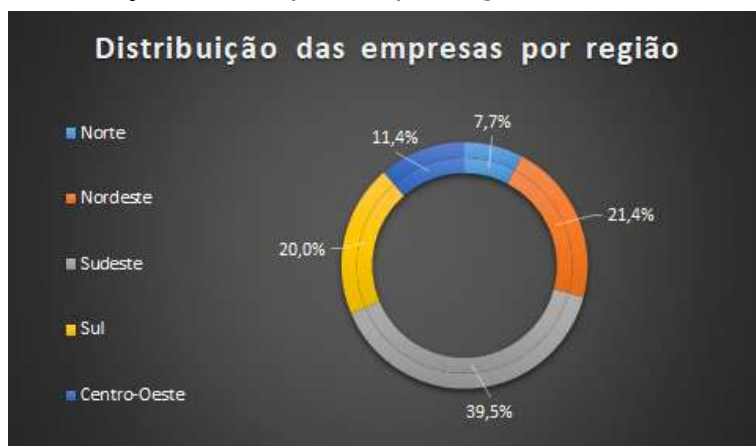
Fonte: http://www.fenavist.com.br/static/media/essegs/ESSEG_V.pdf

O crescimento do número de empresas de 2012 a 2016 fica evidente com um percentual percebido que monta a casa dos 12,2%. Apenas no ano de 2016 observou-se uma pequena retração na ordem de 0,8%. Os números são impressionantes e mostram que o mercado de fato é sólido e viabiliza investimentos dos empresários do ramo. Essa retração ocorrida em 2016 teve início em 2015 e deveu-se ao fato de que este ano foi considerado o pior do ponto de vista do cenário econômico e o país passou por uma das maiores recessões da história, segundo especialistas. Disponível em: <<https://www.valor.com.br/brasil/4890204/pib-do-brasil-recua-36-em-2016>> Acesso em: 10/02/2019.

Se considerarmos as informações e avaliações mercadológicas, podemos então ratificar que o segmento apresenta solidez e credibilidade, pois foi um dos setores que respondeu bem ao cenário imposto ao mercado naquele ano e seguiu forte nos anos seguintes, não somente por razões econômicas, mas pelas questões de fragilidade na segurança pública em diferentes regiões do país.

Não por fatores estatísticos de criminalidade, mas por ser a região onde se encontra a maior parte da população do País, o Sudeste concentra o maior número de empresas não só na atividade de vigilância, mas também na atividade de transporte de valores e cursos de formação. Nessa região, e nessas atividades, o estado de São Paulo, sozinho, representa cerca de 57,7% do total de empresas.

Distribuição das empresas por região



Fonte: http://www.fenavist.com.br/static/media/essegs/ESSEG_V.pdf

O estado de São Paulo é considerado a meca do mercado de segurança privada no país e lá estão concentradas, não só a maioria, mas também as mais qualificadas e maiores empresas do Brasil possuem suas sedes no Estado. Outro fator diretamente ligado a área, no quesito qualificação, é que São Paulo também abriga grandes escolas de treinamento profissional que foram impulsionadas pelo fortalecimento deste segmento, o que destaca ainda mais o mercado paulista. Somente o braço da segurança patrimonial conta com mais de 500.000 colaboradores registrados e, assim como a concentração de empresas, a maioria destes profissionais está alocada no Sudeste do Brasil. É uma relação clara, haja vista que as cidades que compõem a região abrigam a maioria das empresas e escolas de capacitação.

Distribuição dos trabalhadores por região



Fonte: http://www.fenavist.com.br/static/media/essegs/ESSEG_V.pdf

O perfil de mão-de-obra da categoria passou por poucas mudanças ao logo destes anos. No primeiro período a exigência para ocupar o cargo de profissional de segurança era definida pela robustez; a compleição física era o principal critério. A baixa escolaridade predominava, mas ainda não se destacava negativamente no cenário da época, pois segurança era uma atividade que nascia nas empresas que eram fiscalizadas pela antiga Secretaria de Estado de Polícia Civil, onde os vigilantes tinham direito a carteirinha do DSOS após o cumprimento de uma pequena carga horária na ACADEPOL, fato que atribuía certa importância a quem ocupava o cargo.

A partir dos anos 90 o Brasil obteve estabilidade financeira e as pessoas passaram a ter noção do quanto valia seu dinheiro e o mundo entrava na era da qualidade total, o que obrigou as empresas as exigências para admissão dos novos profissionais, o que foi ratificado pela Portaria 992 de 25 de outubro de 1995, que regulamentou um curso de carga horária de 120 horas e previa reciclagens a cada 24 meses. O perfil que temos hoje, nasceu neste ponto e a segurança privada que, ontem era um mercado carente profissionalização, seguiu se expandindo e se transformou em um celeiro de oportunidades.

Este é um segmento que nasceu no meio do caos vivido pela sociedade no fim do período do Governo Militar, que opera com doses altíssimas de pressão e stress potencializados por fatores externos que, em momentos extremos, fogem ao controle de qualquer estratégia, requerendo dos profissionais cada vez mais estudos dos fatores e não só o cumprimento dos protocolos inerentes exigidos pela legislação vigente. Se antes apoiava-se no critério compleição física como fator de escolha para a ocupação deste cargo, o mercado em evolução, principalmente em razão dos cenários impostos, exige muito mais do que a capacitação estabelecida pelo Departamento de Polícia Federal, órgão responsável pela fiscalização da categoria em nível Brasil. São estes, a saber:

- ✓ Curso de Formação de Vigilantes;
- ✓ Extensão em Transporte de Valores;
- ✓ Curso de Extensão em Escolta Armada;
- ✓ Extensão em Seg. Pessoal Privada;
- ✓ Curso de Extensão em Equipamentos Não Letais;
- ✓ Curso de Extensão em Equipamentos Não Letais; e
- ✓ Curso de Extensão de Segurança em Grandes Eventos.

Poderíamos considerar, sem qualquer dúvida, pouco conteúdo para um profissional que, além das atribuições de preservação de vidas e patrimônio, deve, entre outras, gerenciar conflitos inerentes ao ambiente em que atuam, atender as demandas de clientes com relação a dúvidas e insatisfações imediatas, pois muitas vezes é o primeiro profissional a ser visto pelos reclamantes, recebendo toda a carga de stress de uma só vez. Tais constatações foram divulgadas por pesquisa realizada pela pontifica Universidade Católica de Minas Gerais (PUC MINAS) retratando o cotidiano maçante dos vigilantes no estado. Disponível em: <<https://reporterbrasil.org.br/2010/10/cotidiano-de-vigilantes-e-marcado-por-pressao-fisica-e-psicologica/>> Acesso em: 10/02/2019.

Os pesquisadores focaram o estudo nos vigilantes que atuam no transporte de valores, mas também coletaram informações em áreas como

indústria, eventos e setor bancário, ou seja, a gama de entrevistados foi a mais diversa possível. Os problemas comuns a todos os vigilantes foram, entre outros, desgaste mental, traumas psicológicos e doenças ligadas ao sistema nervoso.

Embasada em 5.076 questionários, a pesquisa promoveu um “mapeamento socioeconômico sobre as condições de trabalho e saúde dos vigilantes do estado mineiro, como uma visão geral deste profissional”, segundo a chefe do centro regional da Fundacentro, Marta Freitas. A atividade identificou que 85% dos pesquisados disseram sentir dor nas pernas e mais de 35% disseram ainda ter realizado algum tipo de tratamento de saúde, ou seja, assim como outras atividades que submetem o trabalhador a condições de extrema pressão e stress, podemos considerar que a segurança patrimonial está no rol das atividades laborais com muito mais ônus do que bônus, oferecendo inclusive, iminente risco a vida.

Seguindo uma linha de estudo diferente, porém oferecendo orientação de como os profissionais da área podem evitar alguns males atribuídos a esta atividade, o site da escola de segurança tipifica 06 tipos de doenças e oferece dicas de como evitar certas patologias inerentes. Disponível em: <<https://blog.escoladeseguranca.com.br/doencas-dos-profissionais-de-seguranca-e-como-evita-las/>> Acesso em: 10/02/2019. O site, assim como a pesquisa da universidade mineira, faz o link entre o tipo de exposição sofrida pelos agentes de segurança privada e as doenças mais corriqueiras observadas quando os vigilantes são afastados de suas atividades.

Visto que todas as assertivas se baseiam em pesquisas respaldadas por metodologia e dados estatísticos de institutos ligados a categoria, o que se pode concluir é que se trata de um segmento complementar a segurança pública e, a cada dia que passa, ganha mais importância na proteção à vida e aos bens da sociedade brasileira, pois age de forma preventiva contribuindo para a diminuição da criminalidade. Hoje, a maior parte dos governos enxerga a segurança privada como parceira da segurança pública e não como concorrente. Em alguns países é responsável inclusive pela segurança de bases militares.

É correto afirmar que a segurança privada jamais irá exercer o “poder de polícia”, mas se torna cada vez mais um instrumento fundamental de apoio ao Estado na prevenção de crimes e vem se consolidando como importante protagonista na proteção de vidas e patrimônio das organizações públicas e privadas.

André Vicente dos Anjos, Ph.D., C.P.S.I., C.I.G.R.,C.I.S.I,DIDS – Doctor Of Philosophy In International Security Sciences, Ph.D. – Cambridge Internacional University; Especialista em Segurança Pública e Privada; Especialista em riscos corporativos; Docente e Sócio Honorário CEAS-INTERNACIONAL.

UM RAIOS X DA CRIMINALIDADE NO BRASIL

É de comum sabença que grande parte do conteúdo disposto nas diferentes mídias versa sobre violência. Como pauta predominante, a mídia tem arremessado sobre a população, doses cavalares de desesperança por dias melhores. Não por acaso, mas os números são preocupantes e mostram a cronicidade e a crescente escalada da violência em todo o território nacional.

Algumas das principais pesquisas realizadas nos últimos anos mostram, em números, o cenário do Brasil no que tange a problemática da violência. Por exemplo, o IPS que é elaborado pela da organização sem fins lucrativos **Social Progress Imperative** cujos dados estão divididos em três grupos: necessidades humanas básicas, fundamentos de bem-estar e oportunidades. Cada um contemplando quatro indicadores de qualidade. No índice geral de qualidade de vida o Brasil ocupa o vergonhoso 45º lugar. Disponível em: <<http://g1.globo.com/mundo/noticia/2014/04/brasil-e-o-11-pais-mais-inseguro-do-mundo-no-indice-de-progesso-social.html>> Acesso em: 10/02/2019. A violência é o principal item que puxa para baixo o desempenho do Brasil em qualidade de vida, de acordo com dados do relatório Índice de Progresso Social (IPS). Entre os 132 países analisados pelo documento, o Brasil aparece na 122ª posição no ranking de segurança pessoal, ou seja, considerando o final do ranking como o de país mais inseguro, o Brasil aparece em 11º lugar.

Da mesma forma, o **ExpatInsider** realizou a mais abrangente pesquisa sobre vida no exterior e parte do seu conteúdo foi divulgado pelo site Forbes UOL. Disponível em: <<https://forbes.uol.com.br/colunas/2018/09/brasil-o-lugar-mais-perigoso-para-se-viver-diz-estudo/>>. Acesso em: 10/02/2019. Em resumo, a pesquisa mostra que o Brasil não é considerado um lugar seguro pelos imigrantes, que também criticam a infraestrutura e o cenário político desfavorável para a permanência no país.

Os tipos criminais observados nos últimos anos mostram que existe um caráter de sazonalidade nas diferentes ações criminosas, ou seja, existe uma clara prática predominante durante determinado período que ganha grande destaque da mídia e parece ditar ou motivar ações iguais em diferentes pontos. Quem não se recorda da grande onda de assaltos a agências bancárias país afora, com ênfase em capitais como Rio de Janeiro e São Paulo, obrigando o aperfeiçoamento de grupos de policiais especializados de vários estados da federação.

Outra grande modalidade criminosa também ganhou destaque na mídia durante meses foi o sequestro de empresários, banqueiros e executivos de empresas e tirou o sono das autoridades durante um longo tempo. As ações de grande vulto seguiram esta trilha passando pelos assaltos as casas lotéricas, explosões de caixas eletrônicos até chegar a vez dos shopping centers. Claro que nunca se deixou de praticar crimes distintos em diferentes locais, mas algumas destas modalidades ganharam maior destaque das diferentes mídias.

Mais recentemente, seguindo esta espécie de sazonalidade mórbida, o roubo de carga assumiu seu destaque temporal. O site EXAME divulgou recente matéria levantando dados estatísticos em nível Brasil e mundial. Disponível em: <<https://exame.abril.com.br/negocios/dino/brasil-ocupa-lista-de>>

países-com-maior-índice-de-roubo-de-carga/> Acesso em: 10/02/2019. Segundo a pesquisa o país ocupa o sexto lugar como um dos mais perigosos neste quesito, situação que inflaciona o mercado, elevando os valores de seguros a níveis jamais vistos para este serviço.

Estatísticas de roubo de cargas por região



Fonte: <http://www.setcesp.org.br/servicos-operacional/ntc-divulga-estatistica-de-roubo-de-cargas-em-2017/28797>

Outro importante elemento da mídia eletrônica, o site do estado também divulgou relevante matéria com a mesma temática. Disponível em: <<https://estradao.estadao.com.br/caminhoes/roubo-de-carga-ultrapassa-prejuizo-de-r-15-bilhao/>> Acesso em: 10/02/2019. A matéria pontua que o prejuízo com roubos de carga cresceu 49% nos últimos anos com um prejuízo financeiro que está na ordem de R\$ 1,5 bilhão.

Aparenta ser uma coincidência, mas ao passo que a região sudeste abriga a maioria das empresas de segurança privada e, conseqüentemente o maior número de profissionais, as estatísticas apontam que a região é a mais afetada pelas ações predatórias e a que apresenta o maior índice de crescimento em determinados tipos criminais.

Em 2018, o Instituto Igarapé divulgou uma ampla pesquisa com dados estatísticos que descortinam o real cenário da segurança pública do ponto de vista de infraestrutura e os números apresentados confirmam a desconfiança dos brasileiros na crença de que a situação está longe de ser resolvida. Além de revelar dados desanimadores sobre a ineficácia do Estado, o Instituto apresenta algumas boas sugestões a serem implementadas nas diferentes áreas em que a pesquisa teve seu foco. Disponível em: <<https://igarape.org.br/7-passos-para-vencer-o-crime-em-todo-o-brasil/>> Acesso em: 10/01/2019.

Um dos tópicos da pesquisa ressalta a importância do poder do Estado e de seu aparato no combate à criminalidade e faz um comparativo entre Brasil e Estados Unidos, ponderando sobre o empenho do aparato para este fim.

Comparativo de empenho Estatal:



Fonte: Bureau of Justice Statistics, Instituto Cidade Segura e Ministério de Planejamento

Os dados também mostram que o Brasil é um país que investiga pouco e resolve menos crimes que as grandes potências econômicas do mundo. Um fato que agrava ainda mais este cenário é a falta de um banco de dados unificado. São diferentes órgãos emissores de documentos, cada um com seu respectivo banco de dados.

Comparativo de resolução de crimes:



Fonte: Criminologista Tulio Kahn, Instituto Cidade segura e Sou da Paz

Corroborando com informações contidas nas pesquisas e matérias contempladas no estudo, o fórum brasileiro de segurança pública divulga, através de seu anuário, divulga uma compilação de dados estatísticos com um raio X do cenário e, de fato, os mesmos índices de crescimento assustadores de outros anos se mantêm, o que comprova a ineficácia do Estado na tratativa deste importante tema. Uma das tentativas mais equivocadas de frear a violência no país foi a implantação do ESTATUTO DO DESARMAMENTO, uma experiência frustrada de redução dos níveis de violência sem a amplitude necessária para tal. Um projeto frágil que, no primeiro momento, contou com a adesão dos brasileiros, mas logo se mostrou ineficaz, pois não conseguiu atingir seu principal objetivo.

Anuário de segurança pública



Fonte: <http://www.forumseguranca.org.br/publica/>

De acordo com a justificação da norma, o projeto foi uma resposta do Senado a onda de violência que vinha se avolumando no país, que tinha como uma de suas principais causas a facilidade de obtenção e uso de arma de fogo, pressupostos de fato alegados para sua criação (BRASIL, 1999).

A relevância social do Estatuto constituía-se na expectativa de conter ou fazer retroceder os atos que assolam diariamente a sociedade brasileira de forma gradativa e que aparenta incontrole em relação aos índices de criminalidade já vistos. A realidade devastadora preocupa visto que os crimes continuam sendo praticados por indivíduos portando arma de fogo e os números são crescentes.

Destarte, a sociedade oprimida pela criminalidade entende que aplicação do estatuto não se mostrou eficaz sob o ponto de vista de resultados, demonstrando de forma clara que apenas o cidadão de bem cumpre o dispositivo legal e perdeu sua prerrogativa do direito de defesa. A legislação que proíbe e burocratiza a aquisição ou porte de arma de fogo por civis não atendeu aos anseios dos milhões de brasileiros que apoiaram a regra via plebiscito e ainda restringiu para os civis proponentes o Direito de porte nos ditames da Lei, pois o requisito “demonstração de efetiva necessidade” constitui-se num dos maiores empecilhos para o cidadão que deseja utilizar a arma de fogo como meio de defesa, pois sujeita-o à discricionariedade do Estado e a subjetividade de seus representantes, tanto para a concessão de autorização de compra da arma de fogo como para obtenção da licença de porte (QUINTELA; BARBOSA, 2015).

A Câmara dos Deputados apresentou razões mais condizentes para a justificar o estatuto através do relatório do Deputado Luiz Eduardo Greenhalgh (2003, p. 3). Segundo o referido parlamentar, a Lei n. 10.826/2003 se fazia extremamente necessária em razão da grande quantidade de armas de fogo no Brasil, em sua maioria armas de pequeno calibre. Estudos da ONU teriam mostrado que 80% dos homicídios do país eram praticados por armas dessa natureza, notadamente revólveres. Ademais, acrescentou que 78% das armas apreendidas pela polícia à época seriam procedência nacional. O raciocínio empregado pelo relator foi o seguinte: a diminuição da quantidade de armas nas mãos do cidadão comum levaria à redução na quantidade de armas nas mãos dos criminosos, e, portanto, à redução da criminalidade. Vejamos:

[...]E, se levarmos ainda em consideração que as armas atualmente nas mãos dos criminosos, em grande parte, são as que um dia foram legais e que foram roubadas ou furtadas, chegaremos à conclusão de que uma diminuição geral de armas legais poderá ocasionar também uma queda na quantidade de armas ilegais em circulação, se essa demanda não for suprida pelo contrabando (GREENHALGH, 2003, p. 5).

Não obstante o intento do referido texto legal, hoje é possível perceber de forma inequívoca a ineficácia do Estatuto do Desarmamento e, mais ainda, pela descrença da sociedade, opina-se que o plebiscito conseguiu adesão em percentuais tão altos por conta do grande dispêndio de propaganda do governo

aliado aos crescentes índices de violência na época. Essa era a alternativa predominante e não encontrou oposição em razão do cenário de violência que perdura até hoje em níveis cada vez mais assustadores.

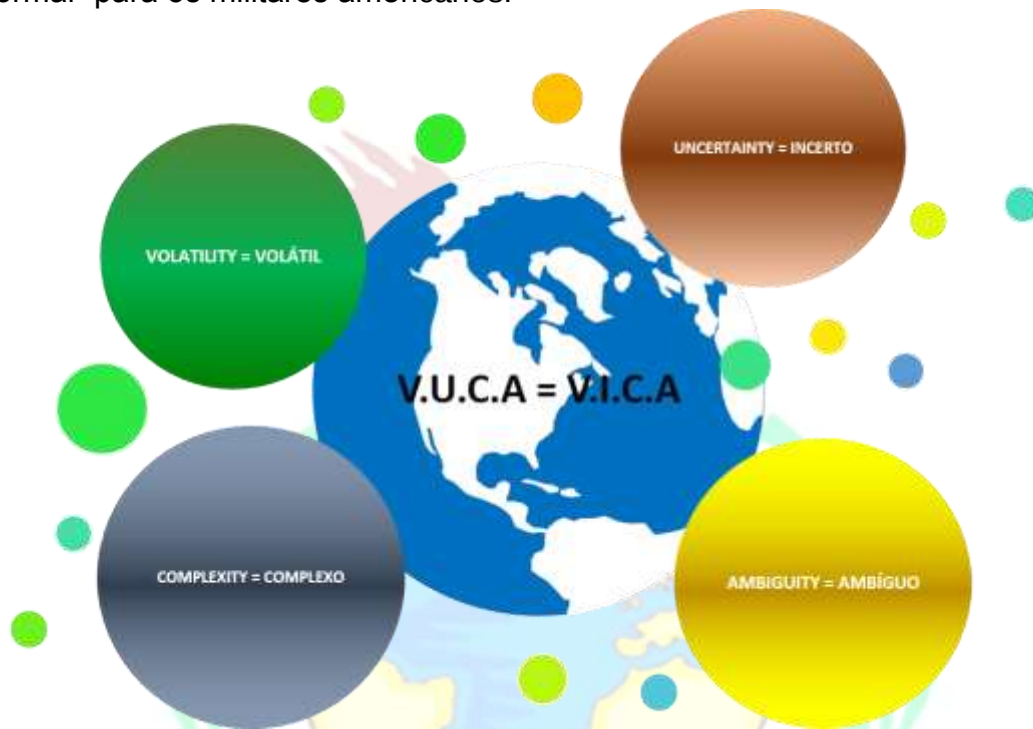
André Vicente dos Anjos, Ph.D., C.P.S.I., C.I.G.R.,C.I.S.I.,DIDS- Doctor Of Philosophy In International Security Sciences, Ph.D. – Cambridge Internacional University; Especialista em Segurança Pública e Privada; Especialista em riscos corporativos; Docente.



SHOPPING CENTER – OS NOVOS RISCOS

O mundo **V.U.C.A**, sigla advinda do contexto militar Norte Americano, busca descrever os desafios nos mais diferentes cenários de guerra em todas as suas nuances e, desde o final dos anos 90, integra um conjunto de ferramentas e métodos criados para fazer frente ao ambiente extremamente adverso, agressivo e desafiador.

Hoje, os contextos que envolvem esta sigla fazem parte do novo “normal” para os militares americanos.



Sendo o mundo corporativo desafiador, agressivo, competitivo, volátil e cheio de incertezas, não se pode dissociar esta sigla dos cenários inerentes ao ambiente empresarial. Neste sentido, um dos ambientes que sofre grande influência dos efeitos deste mundo **V.U.C.A** são os shopping centers, pois trata-se de um de um espaço aberto ao público com o grande objetivo de ser um atrativo aos clientes de diferentes classes sociais e com os mais complexos comportamentos. Tal situação condiciona repentinas mudanças de cenários e essa nova perspectiva exige do especialista em riscos, um olhar mais holístico do negócio, sem deixar de lado os riscos inerentes, sempre considerados na análise do empreendimento.

Hoje, com o advento dos grandes debates de cunho político partidário, por exemplo, riscos antes considerados com baixa probabilidade de materialização deixaram de ser coadjuvantes para ocuparem papel de destaque, gerando grande preocupação em razão dos impactos que podem causar. Esses grandes movimentos sociais têm gerado grande repercussão nas diferentes mídias e arrastando multidões, ocasionando enormes concentrações de pessoas em locais públicos.

Além de um cenário político ainda instável, o país vive momentos de grande mudança por conta de uma nova forma de comunicação. Isso mesmo. A forma de se comunicar não é mais a mesma e os impactos sociais promovidos pelos meios de comunicação atuais são imensuráveis. Pode se

saber de tudo em tempo real em qualquer parte do mundo e uma frase dita de forma impensada por um profissional que vive no ambiente corporativo pode causar danos irreparáveis a imagem de uma empresa que demorou anos para se estruturar.

Como esses novos cenários, trazidos à baila pelo mundo **V.U.C.A**, afetam os grandes centros de varejo no contexto da gestão de riscos?

O primeiro grande impacto causado pelo mundo **V.U.C.A** é o de dificultar planejamentos de médio e longo prazo obrigando as organizações a buscarem maior agilidade e menos burocracia, eliminando processos que não agregam e que possibilitem respostas mais rápidas e assertivas. O empoderamento da ponta é salutar, pois viabiliza melhores ações para vencer no mundo volátil, incerto, complexo e ambíguo. Os profissionais da segurança necessitam desenvolver ainda mais habilidades como inteligência emocional, resiliência e criatividade para sobrepor as ameaças. Alguns dos riscos que assumiram protagonismo dentro deste contexto são:

1) Grandes aglomerações de pessoas

Esse risco é tipicamente atrelado aos grandes movimentos sociais percebidos no ambiente externo, mas seus desdobramentos podem facilmente afetar um grande centro comercial que esteja nas proximidades, caso exista hostilidade entre os manifestantes.

2) Intolerância ≠ Preconceito

Recusa de determinado pensamento, ação ou da convivência com determinados grupos sociais. Reação baseada na não aceitação. “Eu não aceito e demonstro minha reação”.

3) Pedintes ou presença de moradores de rua

O ato ou ação de pedir está diretamente ligado a fatores (externos) sociais. É uma ocorrência que tem se tornado recorrente nos centros de varejo país a fora.

4) Presença de animais perdidos

É comum encontrar animais perdidos nos pátios e estacionamentos dos centros de varejo. A forma como essa situação for conduzida pode gerar grande repercussão, tanto positiva como negativa.

5) Rolezinho

É um neologismo aplicado a uma ação conjunta de passeio em grandes grupos ou encontros simultâneos. Esses movimentos causaram grande impactos nos shoppings recentemente.

Se antes era um tabu para profissionais da segurança acompanharem as mídias sociais, hoje, com a comunicação ocorrendo extremamente rápida através destes novos elementos, se tornou essencial o monitoramento deste universo a fim de criar estratégias personalizadas, assertivas e que minimizem os impactos massivos ora observados diante de materialização de riscos com este perfil.

Como exemplo recente, podemos citar o caso de uma grande rede de supermercados amplamente afetada pelo cometimento de uma conduta equivocada por um de seus agentes, fotografado infringindo maus tratos a um cachorro que parava com frequência na porta do estabelecimento. Além da imagem arranhada pelo fato, foram milhões em prejuízo financeiro, haja vista a evasão de clientes solidários a causa da proteção dos animais. Poderíamos

citar inúmeros outros casos que ganharam grande vulto graças aos novos meios de comunicação, sua velocidade, alcance massivo e imprevisível, um dos efeitos do mundo **V.U.C.A.**

Neste sentido é importante considerarmos a criação de cenários que permitam ao empreendimento preparar suas defesas de forma estruturada e, quem sabe, com o devido gerenciamento, mudar o status deste risco materializado que, ao invés de perdas, pode gerar ganhos. Segundo Brasiliano (2016, p. 06), o conceito mais atual de risco envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às “perdas” como aos “ganhos”, com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organização.

Ademais, os grandes empreendimentos devem focar seus esforços, não apenas na identificação, análise e tratamento dos riscos, mas nos seus impactos, pois certos riscos materializados podem gerar uma crise, ainda que de pequeno vulto.

O gerenciamento de uma crise, pequena, média ou massiva não deve ficar nas mãos de um único profissional, justamente pelos diferentes níveis de impacto que esta pode causar e pela extensão dos danos, que só podem ser mensurados pelos gestores dos diferentes departamentos, possuidores das informações pertinentes a cada área da organização, pois além dos impactos operacionais, que permitem, em determinados cenários, correções, devemos considerar com o devido peso os seguintes danos:

IMAGEM = MARCA

Trata-se de um bem intangível. Não há como mensurar os danos causados a determinada marca quando esta é afetada por um risco materializado, cabendo ao departamento responsável (Marketing) implementar as contingências definidas para minimizar os impactos, bem como a preservação da marca e a continuidade das atividades.

LEGISLAÇÃO = REQUISITOS LEGAIS

A responsabilidade pelos atos de seus agentes e/ou prepostos é do empreendimento. Essa responsabilidade pode ser DIRETA ou INDIRETA, quando o empreendimento responde de forma solidária pela prática de atos de terceiros contratados. É comum perceber os departamentos Comercial e Jurídico envolvidos nas respostas diante da existência de impactos que envolvam questões legais.

FINANCEIRO = PREJUÍZOS / RESPONSABILIDADE CIVIL

A reparação de dano (INDENIZAÇÃO) após o processo transitado em julgado pode ser financeira ou substituída por uma medida compensatória, mediante acordo entre as partes, ratificada por um juiz de Direito. Da mesma forma, os Gestores deste departamento devem atuar em estimativas e mensuração das possíveis perdas financeiras ocasionadas pelo risco materializado.

Além dos inúmeros exemplos de conhecimento público e alcance nacional, temos aqui uma base estruturada para que o entendimento dos

conceitos de gerenciamentos de riscos seja ampliado dentro das organizações, de modo que todos os departamentos tenham seus processos mapeados com seu devido crivo e nível de criticidade, bem como suas contingências personalizadas.

Em um panorama como este, onde as informações reverberam em uma velocidade nunca antes vista sem qualquer juízo de valor que pese seus impactos, é preciso manter-se em alerta máximo, com planejamentos de curto prazo, pois estamos de fato no **MUNDO V.U.C.A**, ou seja, vivemos em uma grande **MUVUCA** que muda cenários em uma fração de milésimos de segundo, exigindo dos profissionais a capacidade de se reinventar para sobreviver e ter êxito neste cenário desafiador, inóspito e cheio de riscos.

Dr. André Vicente dos Anjos, Ph.D., C.I.G.R. – Doctor Of Philosophy In International Security Sciences, Ph.D. – Cambridge Internacional University; Especialista em Segurança Pública e Privada; Especialista em riscos corporativos; Coordenador de Segurança Sênior; Docente. Sócio Honorário CEAS-INTERNACIONAL.



CONJUNTURA E ALTERNATIVAS PARA A SEGURANÇA

O Brasil esta em destaque no cenário da violência urbana e é de conhecimento internacional, uma lamentável constatação e coloca nossos profissionais da segurança pública entre os que mais matam e morrem no mundo dito civilizado. Algo está errado! É urgente a reestruturação do sistema de atuação das nossas polícias, sob pena de não mais conseguirmos reparar tamanha mortandade de pessoas, sejam estas, profissionais da segurança ou outros cidadãos do bem ou do crime, bem como inocentes expostos a escalada da violência.

Neste contexto, deparamo-nos com os serviços de segurança privada, hoje comprovadamente uma força com efetivo que supera as forças de segurança pública e, guardadas as proporções, com o aparato tecnológico considerável a disposição dos órgãos públicos quando solicitado, o que vem em auxílio ao setor público em forma subsidiária e de complemento, contribuindo para a resolução de ilícitos no decorrer das operações em que os órgãos de segurança pública se deparam com suas limitações em termos de equipamentos e até mesmo de efetivo.

Pelo exposto, se pode justificar a reivindicação junto às autoridades, que se oficialize e publique-se a partir das necessárias discussões, a fórmula a ser adotada e operacionalizada com o principal objetivo de prevenir, reduzindo a violência que hoje a sociedade está exposta. Dito no início deste artigo que é urgente a reestruturação das nossas polícias, assim o é a necessidade para a segurança privada, não sendo mais possível compreender de que maneira operacionalizar um 'case' sem a utilização de ferramentais disponíveis em conformidade ao século do conhecimento.

Presenciamos no dia a dia as ousadas operações dos criminosos que planejam suas exitosas operações saqueando valiosas cargas dos carros fortes, instituições financeiras e aeroportos entre outros. Lamentamos a perda da vida destes profissionais que são muitas. Enquanto isso valores que bem poderiam servir a própria segurança, educação, saúde e desenvolvimento geral, estão sendo desviados para atender interesses de quem comanda o crime no Brasil e no mundo.

Este é o debate que requer mais esclarecimentos e, sendo assim, que sejam apresentadas sugestões para a melhoria de tais serviços bem como na preservação das vidas mencionadas. Pois Bem!

- 1) Urge que sejam revisados: Formação, *modus operandi* para abordagens armamentos, munições, treinamento e valorização dos agentes, sejam estes públicos ou privados;
- 2) Que ou profissionais não mais necessitem de 'bicos' para o complemento de seus parques salários;
- 3) Seus períodos de folga possam ser estilizados para o bem estar familiar, desenvolvimento intelectual, saúde física e menta entre outros;

Independente do mencionado convém seja levado à sociedade, esclarecimentos para que esta possa colaborar com ações de prevenção e comportamento que dificultem a ação criminosa. Só assim poderemos ter uma

vida melhor, mais segura e com menos infelizes a cercar o patrimônio que nos custou suor, lágrimas e, por vezes o sangue do cidadão trabalhador.

Ao analisarmos todos os cenários se constata além das urgências, também as alternativas, ou seja, como fazer para a redução dos ilícitos e isto ocorrerá a medida que autoridades ditas competentes se propuserem a ouvir e praticar as observações recomendadas por estudiosos do tema. Não bastam frases de efeito ou decisões equivocadas a partir de uma simples demonstração de poder contido em um canetaço. Nossa sociedade precisa de adequações aos seus moldes e estas virão não com ideologias e politicagem eleitoreiras, e sim, com profunda avaliação do cenário onde estejamos inseridos.

Enor Almeida - Diretor de Relações Institucionais – CEAS BRASIL/RS; Sócio Honorário CEAS-INTERNACIONAL e Colunista do Portal *Security Help*



LA ASESORÍA DE SEGURIDAD, CON ÉNFASIS EN EL TRABAJO DE LA INTELIGENCIA EMPRESARIAL

Una empresa por su envergadura comercial y por las dimensiones de sus instalaciones debería contar con un ASESOR DE SEGURIDAD, con énfasis en la labor de inteligencia, considerando que la asesoría de seguridad tiene por objetivo el análisis inteligente de la situación particular de seguridad de la empresa, para la detección de las fallas y omisiones en la seguridad y su consecuente toma de medidas que aseguren la protección de la empresa.

El asesor de seguridad trabaja con datos de incidentes pasados y presentes para la comparación con los estudios de inseguridad para la comprensión de la fenomenología de los incidentes de seguridad en la empresa. (Probabilística).

Una de las actividades diarias del asesor de seguridad consiste en evaluar de manera permanente las deficiencias de la seguridad existente, sus vulnerabilidades, los desordenes e incumplimientos para una inmediata solución.

El asesor de seguridad deberá diseñar el plan de seguridad de la empresa, donde en ningún momento deberá abandonarse las normas elementales de seguridad por haberse instalado sistemas tecnológicos y humanos de protección en las instalaciones.

Otro punto importante el asesor de seguridad deberá elaborar las normas para los agentes de seguridad, también el manejo de la seguridad de la información en la empresa como función secundaria (contraespionaje industrial).

La función principal del asesor de seguridad es la labor de inteligencia para conocer:

- La inseguridad en la empresa: (La visión global de la seguridad a través de la confección de los mapas de riesgos)
- La seguridad de la empresa: (La confiabilidad y profesionalidad de los servicios vigentes, el nivel real de confiabilidad y eficiencia de las fuerzas de apoyo externo).
- La guía de seguridad: El conocimiento de los gráficos de contactos de seguridad pública)
- La aplicación de las teorías de seguridad: (Teoría de las ventanas rotas y teoría del riesgo).

La metodología de trabajo del asesor de seguridad contempla el siguiente formato:

1. Caso:
2. Empresa:
3. Estructura:
4. Historial de incidentes de seguridad en la empresa:
5. Ámbito de la empresa: Señalización y medidas.
6. Las instalaciones de la empresa: Señalización y medidas
7. Actividad interna de la empresa: Señalización y medidas.
8. Conclusiones:



AIP Guillermo Albornó Mora, CIEIE, CPSI, CIGR. Delegado CEAS en Paraguay y Miembro Honorario CEAS-INTERNACIONAL.

CEAS

PUNTOS A CONSIDERAR PARA LA LUCHA CONTRA EL TERRORISMO:

Los puntos a considerar en este asunto son:

Estudiar y establecer las causas del fenómeno terrorista es lo primero. Buscar sus raíces es el único camino que puede conducir a una respuesta capaz de erradicarlo algún día.

No hay que equivocarse en este aspecto: La lucha contra el terrorismo no puede quedarse en la superficie solamente, donde ciertamente también hay que actuar, si realmente la voluntad estratégica es terminar con este mal, o al menos, reducirlo a su mínima expresión, hay que tener el coraje de identificar las causas y actuar sobre ellas con gran decisión.

Esto obliga a dar una mirada muy completa a toda la realidad mundial en la que estamos inmersos y a ser muy autocríticos a la hora de analizar nuestros propios actos.

Determinadas preguntas claves debemos hacernos : Qué hicimos y que dejamos de hacer para que el fenómeno terrorista alcanzara su magnitud actual ? El caldo de cultivo donde se ha ido desarrollando, es creación exclusiva de los terroristas o existen también con una o muchas contribuciones nuestras ?.

La región sur del continente americano tiene el deber de estudiar las causas del fenómeno terrorista en su propio espacio. Esto lleva a no considerar con tanto énfasis al terrorismo basado en fenómenos menos frecuentes en esta zona, como el generado en el seno del fundamentalismo islámico, por ejemplo, sino a concentrar los mayores esfuerzos en otros ambientes potencialmente estimulantes, como lo son, con seguridad, los fenómenos de desigualdad, pobreza, miseria, exclusión social. Con esto queremos decir que las raíces del terrorismo latinoamericano no están exactamente en el mismo lugar de las que originaron ese fenómeno en otras partes del mundo.

Es necesario y urgente promover el diálogo intercultural para evitar a toda costa un escenario de choque de culturas o guerras santas por ambos lados, que sería catastrófico para toda la humanidad.

Para comenzar por casa en nuestra región latinoamericana y caribenha debemos superar en muchas partes distancias y tensiones, que todavía existen, entre étnias originarias y ese grueso de habitantes que descienden de parte importante de los conquistadores españoles, portugueses e ingleses. La meta debe ser la creación de un ambiente de creciente tolerancia y respeto, capaz de garantizar la convivencia y armonía en sociedades que ya no podrán dejar de ser pluralistas y, por lo tanto, ampliamente democráticas.

El combate al terrorismo no debe cerrarle el paso a las luchas no violentas que, por definición, no recurren al uso de armas que matan.

Este método que en sí mismo reduce drásticamente la violencia en la sociedad y es, por eso, eminentemente antiterrorista, debe permanecer disponible para los luchadores por la libertad, la justicia social y los derechos humanos.

La llamada no violencia activa es el camino para conquistar derechos y para consolidarlos. Este punto es muy importante en las actuales circunstancias, si se quiere tener éxito en el intento de erradicar el terrorismo. Los pobres y miserables, que suman una enorme proporción de la población humana, tienen el más pleno derecho a luchar por salir de su condición y deben disponer de vías pacíficas para hacerlo.

Todo intento de mala fe por confundir la vía no violenta con el terrorismo favorecerá solamente a este último, pues se verá reforzado por aquellos que, en su desesperación e impotencia, no encuentren otra alternativa que plegarse a él.

AIP Guillermo Albornoz Mora, CIEIE, CPSI, CIGR. Delegado CEAS en Paraguay y Miembro Honorario CEAS-INTERNACIONAL.



VOCÊ SABE O QUAIS AS COMPETÊNCIAS PARA SER UM GESTOR DE SEGURANÇA CIBERNÉTICA? O CYBER SECURITY OFFICER – O CSO? NÃO? ENTÃO CORRA, POIS ESTÁ ATRASADO!

Recentemente um relatório da Deloitte do Canadá ressaltou a importância das competências para que uma empresa possua um Gestor de Segurança Cibernética – Cyber Security Officer – CSO para que possa liderar, de forma proativa, com visão de antecipação, tendo a percepção das situações de riscos iminentes, formulando boas estratégias defensivas e tendo planos de reação. Para isso há necessidade do CSO ser DEFENSOR, CIENTISTA, INVESTIGADOR, HACKER, BOMBEIRO, ESTRATEGISTA e ESTRATEGISTA.

O Relatório da Deloitte Canadá resalta que estas competências são dinâmicas, em função do contexto em que estamos vivendo, hoje por exemplo no século XXI, quarta revolução industrial, o mundo é VUCA – Volátil, Incerto, Complexo e Ambíguo, em função desta interconectividade e ao mesmo tempo dinamicidade e o CSO deve possuir como competência:

Ser Defensor - Suportar, administrar e manter a segurança dos sistemas, dados e redes, um viés técnico;

Ser Cientista - Realizar análises especializadas de inteligências de ameaças e informações criptografadas visando melhorar a postura da segurança cibernética da empresa. Neste caso deve possuir uma visão de antecipação, visão prospectiva;

Ser Investigador - Investigar constantemente eventos ligados a cibernética e crimes cibernéticos visando entender o modus operandi e a evolução de ataques que estão acontecendo, além de compreender as evidências e rastros deixados;

Ser Hacker - Realizar atividades especializadas de detecção e decepção de ameaças visando identificar e mitigar os riscos cibernéticos. Pensar como poderiam atacar seus sistemas e de que forma haveria resistência e reação. Pensar como um verdadeiro hacker;

Ser Bombeiro - Identificar, analisar e mitigar as ameaças a sistemas internos, dados e redes. Apagar e anular de forma direta tudo que está colocando em exposição o sistema e informações críticas da empresa;

Ser Estrategista – Fazer gestão, possuir visão estratégica e holística do negócio, implantar indicadores na cibersegurança;

Ser Consultor – Aconselhar e estar sempre up – to – date, com informações atualizadas sobre conceitos, design, sistemas de proteção, construção de sistemas, redes seguras e novas formas de ataques.

O relatório da Deloitte Canadá alerta que as competências mais difíceis de se encontrar no CSO são as de ser Estrategista e Cientista. E que as competências que haverá demandas neste século XXI perante as ameaças serão as de Ser Estrategista, Cientista e Consultor.

O interessante é que as duas mais difíceis e as três do futuro competências possuem como características comuns a visão de futuro, integrada com a visão do negócio da empresa e também a manutenção da atualização do conhecimento.

Portanto na minha visão o CSO deve ser um Nexialista, isso mesmo, nem um especialista nem um generalista. O líder estrategista do século XXI deve ser Nexialista, ou seja, pessoas que movem tudo e todos ao seu redor para atingir seus objetivos. O nexialista é um eterno insatisfeito, eterno curioso, tem o “por quê” no cotidiano e busca sempre formas melhores e mais eficientes de fazer tudo ao redor para fazer acontecer.

O nexialista, líder do século XXI, deve ter habilidade para integrar diferentes matérias ou disciplinas nas empresas, tais como psicologia, química, administração, engenharia, física, entre outras, na busca da solução. Único generalista e integrador processual entre vários especialistas focados em suas respectivas disciplinas, acaba sendo responsável pela solução holística e visão de interconectividade.

O Nexialismo é uma espécie de supra - ciência que integra de maneira sinérgica, complementar e sequencial as várias disciplinas que compõem o conhecimento humano, de modo que as atividades façam nexos entre si. Trabalhando com os paradoxos da consistência e do determinismo, sendo uma abordagem que aproveita os insights gerados por diferentes disciplinas e integra esses insights de maneira que produza resultados exponenciais.

Em um universo de especialização cada vez maior, nada mais importante de ter à visão do todo, poder enxergar a floresta além das árvores. Ser capaz de desenvolver princípios e critérios comuns para o julgamento de nossas ações.

Neste mundo cada vez mais Volátil, Incerto, Complexo e Ambíguo – Mundo VUCA, é cada vez mais importante o líder possuir, não necessariamente a resposta para todas as perguntas, mas a habilidade de saber onde olhar para buscá-las.

Esta é uma nova oportunidade para o gestor de segurança abraçar! Não a perca!

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br

QUAL O PAPEL DA GESTÃO DE RISCOS CORPORATIVOS NA DEFINIÇÃO DA ESTRATÉGIA DA ORGANIZAÇÃO?

A Quarta Revolução Industrial traz consigo um profundo impacto sobre a natureza das relações entre estados e a segurança internacional. Estamos sentindo a incerteza em todas as atividades: concorrentes ágeis e velozes, revolução algorítmica, ambiguidades econômicas no mundo inteiro, sistema financeiro global desestruturado. Estas são algumas variáveis incontornáveis, consideradas como forças motrizes, capazes de alterar os cenários dos inúmeros segmentos empresariais.

A Quarta Revolução Industrial, tecnológica, muda o caráter das ameaças à segurança e, ao mesmo tempo, influencia as mudanças do poder na geopolítica mundial.

As informações e dados são o petróleo do século XXI, onde ideias e pessoas viajam cada vez mais rápidos em um mundo “hiperconectado” e com desigualdades crescentes. Temos Segregação, agitação social que, por sua vez, criam condições para o extremismo violento, ataques cibernéticos em massa. Como conviver com estas ambiguidades?

As empresas pedem por segurança, que é considerada um dos pontos de maior atrito no contexto atual. O medo vende, a insegurança persiste. O que fazer? Não avançar?

Hoje o mundo é considerado Volátil, Incerto, Complexo e Ambíguo, que podemos usar o acrônimo em inglês de VUCA – volatility, uncertainty, complexity e ambiguity nos ambientes e situações de negócios.

Seguindo as premissas do filósofo da Guerra Clausewitz, nunca podemos dogmatizar nossa estratégia, ou seja, torná-la única, aplicando sob a mesma ótica e padrão. A inovação deve ser constante, em função das disrupções do mercado e da concorrência se reinventando o tempo todo, e em constante movimento.

A Gestão de Riscos Corporativos tornou-se um processo primordial, que muitas empresas ainda não se deram conta da sua importância, capaz de subsidiar a Alta Administração na definição das estratégias de negócios, bem como na compreensão e percepção das mudanças de mercado, dos riscos emergentes e disruptivos que podem vir a impactar massivamente a organização. A Gestão de Riscos Corporativos, integrada com a Estratégia Empresarial antecipa ameaças e oportunidades.

Tivemos em 2017, através do novo COSO ERM, Gerenciamento dos Riscos Corporativos – Integrado com Estratégia e Performance, a mudança de patamar para o nível estratégico, onde o risco passou a ajudar na definição das estratégias como na melhoria do desempenho.

A figura abaixo demonstra o Framework da Estratégia integrada com o desempenho, sendo avaliada pelo risco, gerando valor para a empresa:



Definição dos objetivos estratégicos alinhados com a Missão, Visão e Valores, visando a Performance. Fonte: COSO ERM Enterprise Risk Management, Integrating with Strategy and Performance Executive Summary, 2017

O Outro Framework é a operacionalização das fases da gestão de riscos, que mudou radicalmente a abrangência da Gestão de Riscos, ficando extremamente estratégica:



Framework das Fases da Gestão de Riscos, onde o foco passa a ser Objetivos, Estratégia e Desempenho.

O quesito holístico da gestão de riscos é avaliar se a estratégia está alinhada com o apetite ao risco da organização e como ela direcionará a organização na definição de objetivos e alocar recursos com eficiência e eficácia.

A falta desse alinhamento potencializa o risco da organização de não gerar valor, o que pode comprometer seus objetivos e desgastar o valor existente.

Definir estratégia empresarial significa fazer escolhas, fazer o que Michael Porter diz “trade-offs”. A definição da estratégia da empresa deve ser um processo decisório robusto e estruturado, que possua os riscos bem definidos e alinhados com missão, visão e valores.

O Conselho de Administração tem como responsabilidade definir o apetite a risco, além de supervisionar para que este apetite a risco seja base para a definição da estratégia da empresa.

Portanto a Gestão de Riscos é um processo hoje considerado crítico e estratégico para as empresas, não podendo ser negligenciado pela alta administração.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL. abrasiliano@brasiliano.com.br

BRASIL COM GRANDE EXPOSIÇÃO AO RISCO POLÍTICO: INTERCONECTA AO RISCO ECONÔMICO!

Hoje a interconectividade entre os riscos é uma realidade pela velocidade dos negócios e também pelas inovações e os próprios negócios disruptivos. O grande desafio do gestor de riscos é manter seu radar focado nos riscos e eventos de maior motricidade, que se materializado podem comprometer os objetivos estratégicos da corporação. O risco político no Brasil, é hoje, um dos mais sensíveis, pois se refere às decisões do governo e de seus atores, legislativo por exemplo, que podem alterar o resultado esperado e o dado valor de uma ação econômica.

O risco político enfrentado pelas empresas pode ser definido como o risco da perda da estratégia, financeira ou pessoal, devido a tais fatores não comerciais, como políticas sociais e macroeconômicas, de ordem fiscal, monetária, comercial de investimento, industrial, renda, trabalho e de desenvolvimento. Temos também o lado relacionado à instabilidade política pura, gerando terrorismo, tumultos, probabilidade de golpe de estado, guerra civil e insurreição.

Isso tudo pode ser devido à expansão internacional sem precedentes dos riscos em todo o mundo, os profissionais de risco das corporações devem agora estar preparados para praticamente qualquer tipo de ameaça política ou econômica em mercados desenvolvidos e / ou emergentes.

No Brasil estamos vivenciando o risco político resultante da inércia do Presidente Bolsonaro em não tomar a dianteira para levar aos parlamentares a reforma da previdência. A Reforma da previdência é um fator crítico de sucesso para que o Brasil possa deslançar, o mercado de investidores nacionais e estrangeiros estão na expectativa que esta ação aconteça, ainda neste primeiro semestre.

O governo de Jair Bolsonaro tem que fazer alguma articulação, caso contrário, corre o risco de paralisação ou de simplesmente a reforma da previdência não passar, não ser aprovado na Câmara dos Deputados, o que seria desastroso para o Brasil.

O governo está sendo bombardeado pelas mídias com cobranças sobre sua paralisação, em função do Presidente Bolsonaro não querer entrar no “velho jogo” toma lá da cá, mas terá que conquistar apoio e votos para o projeto da reforma da previdência, tido como impopular. Não tem jeito. Terá que se mexer para não desandar todo o processo de governabilidade.

O clima político brasileiro, nestas últimas semanas azedou ainda mais com as desavenças do ministro da justiça Sergio Moro e o Presidente da Câmara Rodrigo Maia, que resolveu adiar a tramitação do pacote anticrime, ocasionando um desentendimento público entre o ministro e o presidente da câmara. Esta atitude de Maia fez com que houvesse críticas dos Bolsonaroistas nas Redes sociais, inclusive pelo filho mais novo do Bolsonaro, Carlos, que classificou Maia como sendo da “velha política”. Maia chegou a ameaçar de romper de vez, sendo ele um elo importante, pois é o fiador do projeto da reforma da nova previdência.

O segundo tempero azedo foi a prisão de Michael Temer e do ex-ministro Moreira Franco, os dois pela Lava Jato e símbolos da “Velha Política”.

Ressalva importante é que Moreira Franco também foi governador do Rio de Janeiro e é sogro do Presidente da Câmara Rodrigo Maia. Pinta um ar de doce veneno! Será?

Acabou que Maia não rompeu, ou seja, não virou as costas para a reforma da previdência, por sua importância política e econômica para o Brasil e claro, mas também capitaliza bônus em cima deste projeto. O contexto é, na minha opinião, crítico! Pois é responsabilidade do Palácio do Planalto e não do congresso a conquista do projeto.

Maia mesmo assim critica Bolsonaro, afirmando que: “O Presidente da República possui a responsabilidade de conduzir a aprovação da reforma. Ele precisa ter um embasamento maior. Ele precisa ter mais tempo para cuidar da previdência e menos tempo para ficar cuidando do twitter”.

Portanto estamos diante de um grande Risco Político, com consequências massivas para o Brasil, caso a reforma não saia ainda este semestre.

Sem Maia não há reforma. Em dezembro de 2017, depois de uma série de atritos com o então presidente Michael Temer, Maia simplesmente engavetou o projeto da reforma. A proposta não durou e Temer não aprovou mais nada.

O mercado acompanha de forma direta e incisiva o desfecho desta situação. A bolsa de valores de São Paulo, depois de bater o nível recorde de mil pontos no dia 19 de março, fechou o índice Bovespa no dia 22 de março em 93,720, na pior semana desde agosto de 2018. As ações ficaram no vermelho na sexta-feira (dia 22/03), com quedas expressivas em Blue Chips como Petrobrás e bancos. Consequência da instabilidade e indícios de não governabilidade, por parte do presidente Bolsonaro.

Na primeira e segunda semana de abril serão cruciais para o governo conseguir consertar a relação com os parlamentares ou já começaremos em posição de grande desvantagem, pois sem Reforma da Previdência, não tem como o governo Bolsonaro decolar. Simplesmente o Brasil está quebrado. As contas não fecham. Não haverá dinheiro no mercado!

A bancada do governo sequer conseguiu escolher o nome do relator para a reforma da previdência na comissão de constituição e justiça, etapa considerada fácil pelos parlamentares, hoje quando escrevo este ponto de vista, domingo 24 de março de 2019.

Os parlamentares podem, como medição de força, tirar a Polícia Federal da alçada de Sergio Moro ou aprovar um decreto legislativo derrubando a medida do Presidente Jair Bolsonaro que dispensa vistos de turistas dos americanos, retorno da doce vingança. Será?

Outras rugas ainda marcam os parlamentares, tais como o ministro Paulo Guedes, da Economia, não consultou e nem ouviu os políticos antes de anunciar a reforma da previdência.

Na proposta de Guedes tinham dois pontos cruciais, que de cara já eram resistentes e impactariam seus eleitores, o aumento da idade para idosos obterem o benefício do BPC de 65 anos para 70 anos e a obrigatoriedade dos trabalhadores rurais contribuírem por 15 anos para terem aposentadoria.

A outra foi a reforma das pensões dos militares, que não foi enviada junto do projeto dos servidores e trabalhadores civis. Resultado: O congresso parou aguardando a remessa do projeto dos militares.

Foi uma frustração geral, porque juntou dois temas distintos, a reestruturação da carreira militar e a reforma. Aproveitou a reforma e reajustaram os soldos, com a reestruturação de carreiras, incluindo aumento de benefícios na passagem para a reserva, com isso em 10 anos, a economia será de apenas R\$ 10,45 bilhões, um bilhão por ano na inatividade. O militar continuará recebendo todo seu soldo da ativa, enquanto o civil – demais trabalhadores terão um limite que hoje gira em torno de R\$ 5,6 mil. A alíquota previdenciária dos militares é 10,55% e a dos trabalhadores 11% e a dos servidores civis, 14% a 22%.

O projeto da previdência dos militares em termos de comunicação foi um desastre total. Faltou total jogo de cintura para a divulgação, tanto para os parlamentares como para as mídias. A tese vendida inicialmente era que todos os brasileiros teriam que fazer sacrifícios, acabou caindo por terra. Ou seja, há um grande sapo para os parlamentares digerirem e cabe ao Presidente Bolsonaro realizar, com maestria e habilidade, esta difícil tarefa.

A popularidade do Jair Bolsonaro está em queda, o que demonstra que perdeu força popular em um momento crítico. Segundo pesquisa do IBOPE, acendeu a luz vermelha. Os que consideram o governo bom ou ótimo despencou de 45% em janeiro para 34% em março, queda de 11 pontos. Os que avaliam o governo ruim ou péssimo pularam de 11% para 24%. Os que não confiam no presidente passaram de 30% em janeiro para 44% em março. Estamos vivendo um contexto muito conturbado e incerto. O governo precisa agir rápido, muito rápido. Os dois presidentes que perderam apoio por parlamentares, Collor de Melo e Dilma Rousseff, tiveram impeachment. Portanto...olhos abertos...

Torço para que a equipe de JB acorde, rápido e reaja de forma a inverter a situação. A estratégia é uma só, reação imediata, partir para cima dos pontos nevralgicos, caso contrário creio que teremos que amargar um governo na UTI. Espero que isso não aconteça!

Boa leitura! Sorte e Sucesso para todos!

Antonio Celso Ribeiro Brasileiro - Publisher da Revista Gestão de Riscos e Presidente da Brasileiro INTERISK abrasiliano@brasiliano.com.br

em tempo: hoje, 28 de março de 2019, as manchetes dos jornais O ESTADO DE SÃO PAULO e do VALOR Econômico são respectivamente:

“Temor sobre Previdência derruba Bolsa e eleva dólar”

Ida de Paulo Guedes ao Senado não contornou situação; ministro diz não ter apego ao cargo.

“Conflito político atinge mercado e dólar vai a R\$ 4”

Bandeiras estão içadas avisando o Governo de que o contexto político não está nada bem, por esta razão deve reagir rápido e de forma inteligente. Um cenário sem reforma não interessa a ninguém. Mas, fato é, na visão dos parlamentares, é que há grande probabilidade com efeitos massivos, do governo não entregar uma agenda econômica, o significa uma grande

exposição para o Brasil do desequilíbrio fiscal continuar e entrar em stress, levando o Brasil e nós brasileiros a bancarrota!!

Brasil, tenha maturidade e inteligência para reagir, deixe o ego de lado, faça do inimigo o aliado nas horas certas, utilize as técnicas de Sun Tzu, Maquiavel e Clausewitz, faça o Brasil deslanchar economicamente, caso contrário todos nós morreremos na praia!

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br



RISCO DE FRAUDE NO MUNDO CIBERNÉTICO: VOCÊ CONHECE INTELIGÊNCIA ANALÍTICA?

A transformação digital está mudando a maneira como as pessoas vivem e trabalham, conseqüentemente, houve um aumento no volume de dados gerados, estruturados ou não. Com esse grande volume novos riscos apareceram e os métodos tradicionais de prevenção de fraudes não acompanham a velocidade necessária para se adaptar a esse novo cenário. O que fazer?

Soluções poderosas para detectar fraudes em qualquer indústria de Tecnologia a favor da segurança são as denominadas Análises Avançadas e ou Inteligência Analítica.

Quando falamos em Inteligência Analítica na prevenção de fraudes, estamos falando do uso de modelos preditivos, redes neurais (deep learning), análise de links, machine learning e detecção de anomalias. Essas técnicas complementam as estratégias atuais, baseadas em regras de negócios estáticas, e estão em uma tendência crescente, principalmente devido ao novo volume de dados gerado nesta era de transformação digital.

Hoje, os dados são o ativo mais valioso para detectar e evitar fraudes. Embora existam obstáculos como dados em silos, dados de baixa qualidade, fontes diferentes não integradas, falta de recursos humanos analiticamente qualificados, o investimento necessário para ter uma boa estrutura de gestão de dados permitirá transformá-los em valores agregados, seja resolvendo problemas de negócios ou problemas regulatórios. O retorno é garantido tanto na prevenção como na detecção.

Também é importante ter uma ferramenta completa de prevenção de fraudes que ofereça suporte à área de negócios para implementar e integrar a autenticação e possibilitar a Inteligência Analítica. Atualmente, os padrões mínimos que uma empresa deve procurar nesse tipo de solução são:

- Facilidade de integração e preparação de dados para análise;
- Acompanhamento de transações com regras e modelos otimizados que funcionam em tempo real, com uma visão única do cliente;
- Capacidade de geolocalização e análise de ID de dispositivo para contas móveis e digitais;
- Gestão integrada acessível em toda a empresa para dar suporte a alertas e investigações necessárias;
- Visualização de dados por meio de relatórios e gráficos estruturados para a rápida identificação de eventos, atividades ou conexões potencialmente suspeitas.

Os líderes de todos os setores - bancários, seguros, serviços e governo, entre outros - estão trabalhando para simplificar a experiência do cliente com opções de pagamento e serviços online e móveis, fechando as portas da fraude e da exposição. Equilibrar segurança e conforto requer uma abordagem que combine a autenticação voltada ao consumidor com medidas de segurança em segundo plano, como a análise do comportamento do usuário, por exemplo.

O investimento não é pequeno, mas a relação custo benefício, com certeza terá um ótimo equilíbrio.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br



MÓDULO DE NÃO CONFORMIDADES DO INTERISK AJUDA OS GESTORES A ANTECIPAREM RISCOS!

O Módulo de Não Conformidades do Software de INTERISK, possui ferramentas que, quando alimentadas, formam um banco de dados, onde os gestores podem analisar seu contexto, seja ele da segurança corporativa, da segurança do trabalho, da segurança de meio ambiente, segurança em processo, segurança em tecnologia da informação, cibersegurança, e de quaisquer outras categorias de riscos. Serve para qualquer categoria de risco, pois uma não conformidade é um fator de risco, é uma causa de um risco.

Quando o gestor visualiza, dentro de uma moldura de tempo, uma quantidade de Não Conformidades, o INTERISK fornece automaticamente, depois de alimentado, a motricidade do Fator de Risco. Entendemos como Motricidade a relevância da Não Conformidade em potencializar fragilidades para a área ou processo auditado.

A vantagem que a moldura de tempo pode ser desde diária, como semanal, quinzenal, mensal, trimestral, semestral, anual. O gestor escolhe a moldura de tempo para realizar sua interpretação das evidências. Com a visão do todo, o gestor consegue prospectar quais riscos poderão acontecer, em função da relevância das Não Conformidades encontradas.

É de fácil entendimento a lógica estruturada para coletar e transportar para as ferramentas de modo automatizado. Para o gestor, basta a tarefa de realizar a interpretação, ou seja fazer a análise do contexto e verificar qual o grau de fragilidade do ambiente auditado, em função do nível de motricidade das não conformidades.

O primeiro passo é entender que uma não conformidade possui uma classificação em quatro níveis de motricidade: baixa, média, alta e massiva. Para chegar a esta classificação, a Não Conformidade encontrada deve ser analisada sob dois critérios:

- 1) Nível de Influência Do Fator de Risco/Não Conformidade em fazer concretizar os riscos e ou acidentes
- 2) Impacto ou Criticidade dos riscos ou acidentes que este Fator de Risco/Não Conformidade potencializa (tipo de risco em termos de consequência)

O Nível de Influência do Fator de Risco/Não Conformidade pode ser mensurado da seguinte forma:

A equipe do gestor em campo quando encontra uma Não Conformidade perguntará: Quanto que este Fator de Risco/Não Conformidade influencia a materializar os riscos? Quanto que potencializa?

Tem que levar em consideração que um Fator de Risco/Não Conformidade pode pertencer a vários tipos de riscos e o fiscal/auditor tem que identificar seu nível de influência na concretização para cada um deles.

A tabela da nota é:

Nível de Influência	Nota
Influência MUITÍSSIMO	4
Influência MUITO	3
Influência Medianamente	2
Influência Pouco	1

O Impacto ou Criticidade dos riscos ou acidentes que este Fator de Risco/Não Conformidade potencializa (tipo de risco em termos de consequência)

O segundo critério é o Impacto ou Criticidade dos riscos ou acidentes, ou seja as possíveis consequências que este risco ou acidente poderá trazer para a área, processo ou pessoa.

Desta forma a equipe do gestor em campo dará uma nota qualitativa, listando os riscos ou acidentes que podem proporcionar e as possíveis consequências. Com base nos riscos e nas consequências teremos o impacto e ou a criticidade do Fator de Risco/Não conformidade. As notas seguem a tabela abaixo:

Nível de Impacto ou Criticidade	Descritor
4	Fraude, fatalidade e lesão permanente, intrusão no sistema de TI, sabotagem que deixe a empresa descontinuada e outros
3	Acesso não autorizado, sistemas de câmeras sem funcionamento nos pontos críticos, lesões de invalidez temporária e outros
2	Sistema de alarme sem manutenção, falta de capacitação, lesões leves, extintores de incêndio vencido, entre outros
1	Falta de procedimento operacional, capacitação, sem lesão, acidentes com danos materiais, entre outros

Obs: o grande segredo da eficácia é ter um descritor claro e conciso por categoria de riscos, visando dar a equipe de campo uma visão clara e simples para poder classificar.

O Resultado do Cruzamento deste dois critérios é a Matriz de Motricidade, onde o gestor consegue enxergar claramente as deficiências, conforme abaixo:

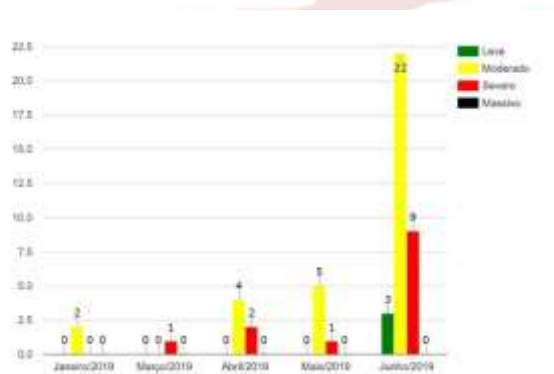


Neste caso temos 49 Não Conformidades – NC na área, sendo 13 consideradas críticas, 33 médias e 3 leves. Não há NC massiva. O tratamento já está direcionado na implantação de controles. O INTERISK pode fornecer outros gráficos automaticamente:

1) Filtragem das Não Conformidades por Motricidade:

Nº	Fator
18	Procedimento de segurança ineficaz ou inexistente.
7	Instalações Elétricas Inadequadas
7	Instalações Elétricas Inadequadas
4	Ferramenta Inadequada
67	Ausência de proteção nos quadros de distribuição ...
1	Ausência de Sinalização
27	Ausência de EPC - Equipamento de Proteção Cole...
22	Posicionamento Inseguro
201	EPC - ausência de proteção coletiva.
292	Escavação Irregular
29	Ato Inseguro/comportamento perigoso
6	Equipamento Inadequado
13	Falta pessoal de manutenção.

2) Não Conformidade por Moldura Temporal e Motricidade:



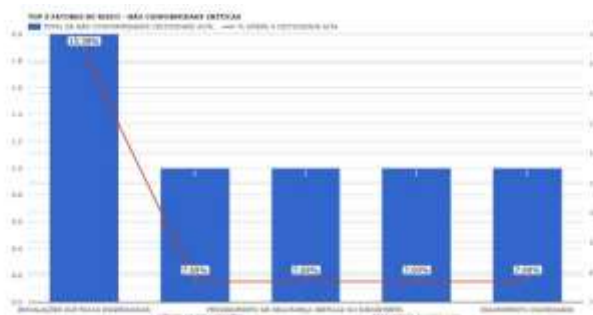
3) Indicador de Motricidade de Tempo x Quantidade

Descrição	Leve	Moderado	Severo	Massivo	Total
Janeiro/2019	0	2	0	0	2
Março/2019	0	0	1	0	1
Abril/2019	0	4	2	0	6
Maior/2019	0	5	1	0	6
Junho/2019	3	22	9	0	34

4) Indicador do Quantitativo das N C Totais x Quantitativas das NC Altas



5) Indicador das Não Conformidades mais Frequentes



6) Cálculo Matemático da Média, Desvio Padrão e Tendência de concretização de determinados riscos ou acidentes

Com estes gráficos e indicadores, os gestores possuem uma visão estratégica e holística da situação da área, processo auditado. Com esta visão o gestor consegue ter antecipação, prevenindo de forma enfática os riscos que podem afetar as operações da empresa e seus objetivos estratégicos. O INTERISK desta forma facilita a vida do gestor, fazendo com que suas equipes fiquem em constante auto verificação e ele sendo alimentado de forma contínua.

MÉDIA ARITMÉTICA	3.00
DESVIO PADRÃO	1.53
COEFICIENTE DE VARIAÇÃO	51%
CHANCE DA MÉDIA SE MANTER	49%
TENDÊNCIA	1.14

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.

abrasiliano@brasiliano.com.br

INTERCONECTIVIDADE E MOTRICIDADE EM RISCOS. O INTERISK AJUDA VOCÊ A ENXERGAR OS RISCOS SISTÊMICOS.

Um dos maiores problemas identificados na área de Gestão de Riscos Corporativos é a não identificação do Risco Sistemico. Você sabe o que é?

Pois bem, O risco sistêmico é o risco responsável por “colapsar um sistema inteiro, oposto de colapso de partes e componentes individuais”. Os riscos sistêmicos são caracterizados por:

- pontos de ruptura modestos, combinando indiretamente para produzir grandes falhas;
- contágio ou compartilhamento de risco, como uma perda que desencadeia uma reação de outras;
- sistemas sendo incapazes de recuperar o equilíbrio depois de um choque.

Isto quer dizer que são riscos que na grande maioria não possuem criticidade alta (resultado da probabilidade x impacto – posição na Matriz de Criticidade), mas possuem grande influência sobre os outros riscos considerados críticos. Na realidade o gestor não enxerga o risco sistêmico porque só elabora a Matriz de Criticidade dos Riscos e com somente esta Matriz fica míope no tratamento e priorização.

Vejamos um exemplo prático: Olhando a Matriz de Criticidade abaixo, o Risco 91 encontra-se no quadrante amarelo, portanto é um risco que está em uma área de monitoramento, não exigindo plano de ação. Correto? Não! Vejamos.

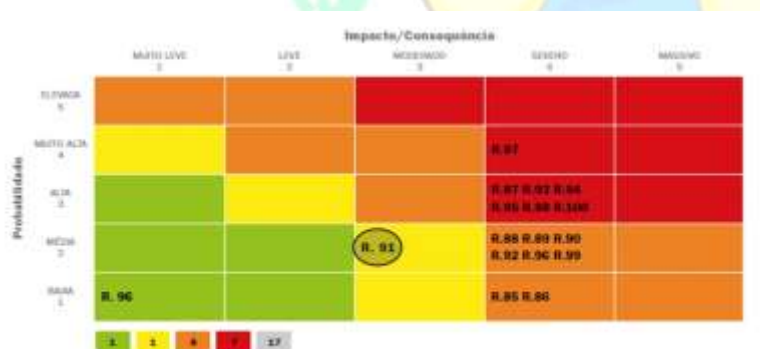


Figura 11 - Matriz de Riscos

Este risco pode ser motriz, ou seja, tem características de influenciar outros riscos a se materializarem. Como podemos saber disso?

Temos que aplicar a técnica dos Impactos Cruzados, Teorema de Bayes – Probabilidades Condicionantes, para identificar Riscos que possuem forte interconectividade motriz com outros Riscos.

Quem pede para utilizar esta técnica junto com a Matriz de Criticidade? O Forum Mundial, em Davos, através do Global Risk Report, sugere a aplicação das duas Matrizes pela área de riscos, visando obter a visão do risco sistêmico. O antigo COSO ERM de 2004, já descrevia a necessidade de realizar a interdependência entre riscos e fatores de riscos. Portanto diante da

dinamicidade do Mundo VUCA – Volátil, Incerto, Complexo e Ambíguo, o gestor de riscos deve aplicar a Técnica de Elaborar a Matriz de Motricidade dos Riscos. Para isso começamos a elaborar a Matriz de Impactos Cruzados - MIC ente riscos, conforme modelo abaixo:

Fatores	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19	R20	Σ
R1	Xa	2	3	3	0	0	0	0	3	1	1	0	0	1	0	1	0	14			
R2	0	Xa	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	3			
R3	3	2	Xa	3	2	1	0	3	3	3	2	2	3	2	29						
R4	3	2	3	Xa	2	2	0	3	1	3	0	0	3	0	22						
R5	0	1	2	2	Xa	3	3	3	3	3	3	3	3	3	32						
R6	0	1	2	2	3	Xa	3	3	3	3	3	3	3	3	32						
R7	0	1	1	1	3	3	Xa	3	2	3	3	3	3	0	3	26					
R8	2	1	1	1	3	3	2	Xa	3	2	3	3	3	3	30						
R9	2	1	2	2	3	3	3	3	Xa	2	3	3	0	3	30						
R10	3	2	3	3	3	3	3	3	3	Xa	3	3	0	3	35						
R11	2	2	3	3	3	3	3	3	3	3	Xa	3	2	3	36						
R12	3	2	3	3	3	3	3	3	3	3	3	Xa	2	3	37						
R13	0	3	2	2	2	3	1	3	1	2	3	3	Xa	3	28						
R14	2	2	3	3	3	3	3	3	3	3	3	3	3	2	Xa	36					
M	20	22	26	28	30	30	24	29	29	31	29	28	22	29	Xa						

Legenda:

1. Baixo Nível de Escolaridade
4. Elevada carga tributária
5. Desigualdade social
6. Exclusão social
7. Corrupção policial
8. Corrupção no judiciário
10. Inteligência Policial
11. Legislação Brasileira
13. Sistema Carcerário
14. Violência Urbana
15. Facções Criminosas estruturação do crime como empresa
16. Facções Criminosas: assistencialismo
17. Valores éticos e morais nas empresas
20. Estruturação das milícias em função da inoperância do Estado.

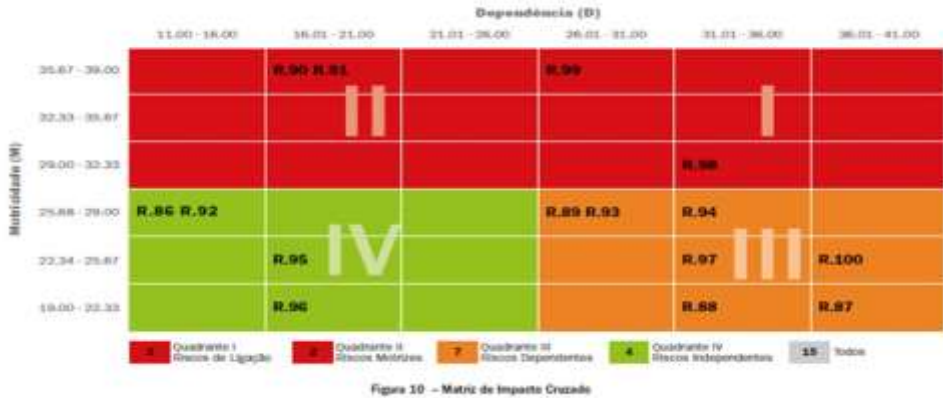
A MIC serve para o gestor enxergar os riscos mais Motrizes e os Mais Dependentes, para montar a Matriz de Motricidade, com dois eixos:
Eixo da Motricidade = Maior Nota de Motricidade + Menor Nota de Motricidade

_____ = Ponto Médio
2

Eixo da Dependência = Maior Nota de Dependência + Menor Nota de Dependência

_____ = Ponto Médio
2

Com isso Montamos a Matriz de Motricidade com quatro quadrantes, conforme abaixo:



Quadrantes:

I – Ligação – Significa que os riscos são dependentes e motrizes, influenciam e são influenciados entre si. Instabilidade, mas influenciam o quadrante III;

II – Motriz – Significa que os riscos são motrizes, ou seja, riscos que influenciam os riscos no quadrante I e III. Estes são os riscos sistêmicos.

III- Dependentes – Significa que estes riscos para serem materializados, dependem dos riscos plotados nos quadrantes I e II. Não adianta tratar este riscos sem antes tratar os riscos dos quadrantes I e II.

IV – Independentes – Significa que estes riscos não possuem interconectividade com nenhum risco. Não tem canal de comunicação. Não significa que não são importantes, são sem canal de comunicação, devendo ser tratados de forma individual.

Se formos ver a Matriz de Motricidade acima, vemos que o Risco 91, que possui uma criticidade baixa, quadrante amarelo, está plotado no quadrante II, é um risco com alta interconectividade motriz. Este risco, embora sem criticidade, é um influenciador para que outros riscos venham a materializar.

O Software INTERISK, único do mercado que possui a Matriz de Priorização, fruto do cruzamento das Matrizes de Criticidade x Motricidade, fornece aos gestores, de forma automatizada, a priorização para tratamento dos riscos, levando em consideração, tanto sua interconectividade como sua criticidade, conforme Matriz abaixo:

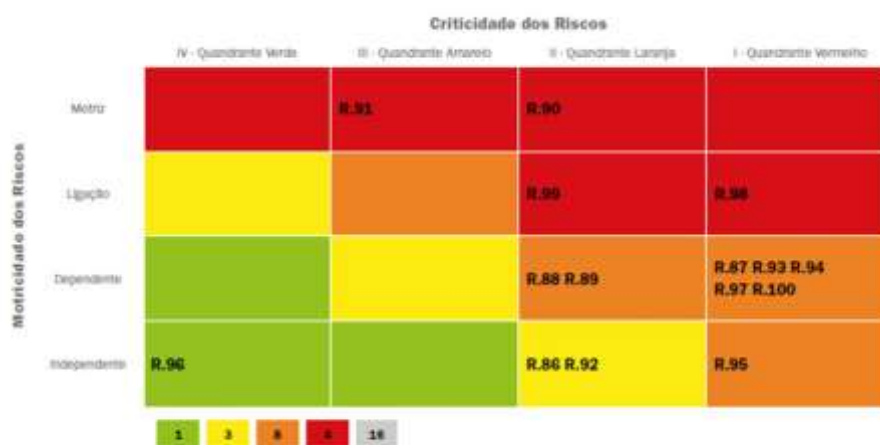


Figura 12 - Matriz de Priorização

A Matriz de Priorização acima, ressalta os riscos sistêmicos, como o Risco 91, que está no quadrante vermelho para ser tratado. Outra vantagem é que otimiza recursos, pois neste caso o gestor de riscos só terá que elaborar planos de ações para quatro riscos. Se por acaso o gestor for tratar um risco que esteja no quadrante laranja antes do vermelho, irá “enxugar gelo”, pois não conseguiu anular a causa raiz.

O Software INTERISK fornece com isso Inteligência em Riscos, agregando valor para o gestor ao prevenir e mitigar riscos sistêmicos.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e

Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.

abrasiliano@brasiliano.com.br



DECEPÇÃO: A ARTE DA CONTRA INTELIGÊNCIA EMPRESARIAL

Nós somos feitos para encarar a uma desgraça mesmo que por falsidade... nós continuaremos a lutar com a convicção que a honestidade é a melhor política e que a verdade sempre acaba vencendo. É um sentimento muito bonito para um livro infantil, mas o homem que se baseia nisso faria melhor se embainhasse sua espada para sempre.

Manual do Soldado Britânico (1869)

Decepção é uma das mais exóticas contramedidas usadas para prevenir a perda de informações sensíveis.

Talvez o estrategista chinês do Século V d.C. disse bem quando sugeriu que: Toda arte de guerra é baseada na decepção. Assim, quando capaz, finja incapacidade; quando ativo, finja inatividade. Quando próximo, faça parecer que você está muito longe; quando longe, que você está muito perto. Ofereça ao inimigo uma isca para atraí-lo; finja desordem e derrube-o. Quando ele se concentrar, prepare contra ele; onde ele for forte, evite. Irrite-o e confunda-o. Finja inferioridade e encoraje sua arrogância.

Estes são os elementos que você quer comunicar para o seu oponente quando você está começando a proteger a si mesmo e quer permitir que ele obtenha impressões errôneas através de seu próprio trabalho de pesquisa. Essas impressões frequentemente gerenciam de tal forma a opinião do adversário que se torna difícil ele acreditar que sejam erradas e sobrepujam muitas vezes as análises mais rigorosas.

Decepção consiste em identificar uma ameaça para a informação de alguém e responder cuidadosamente com informações desenhadas para atingir apenas um receptor, com a intenção de distrair a atenção para longe do que a empresa está realmente fazendo. Fundamental para essa aproximação é criar as condições de erro por parte do concorrente.

Também é importante ter em mente a quantidade de tempo que a empresa necessita de proteção da informação sensível sem comprometer o projeto.

A essência da decepção é saber — ou acreditar que você saiba — quem está obtendo o quê de quem e através de que canais. E então, com esses pensamentos em mente, colocar dentro desses canais — e apenas estes canais — a informação que você quer que eles acreditem e sobre a qual possivelmente irão trabalhar. Desoriente-os até que encontrem um caminho que não mostre o que você está realmente fazendo.

Contudo, um verdadeiramente bem desenvolvido plano de decepção não é simplesmente contar um par de mentiras para algumas pessoas e esperar que alguém da concorrência morda a isca.

A Decepção possui sete mandamentos, que devem ser seguidos para que tenhamos sucesso:

Primeiro Mandamento

Operações de decepção não são nunca organizadas pobremente, jamais devem ser executadas por quem é orgulhoso para precipitar decisões e ter soluções repentinas e decididamente não é para os fracos do coração.

Segundo Mandamento

Antes mesmo de começar um projeto de decepção, pense sobre o efeito de seu programa sobre uma variedade de outros potenciais receptores da informação. Quais serão as consequências. Vale a pena?

Terceiro Mandamento

O número de pessoas que têm qualquer espécie de conhecimento com o projeto de decepção precisa ser o menor possível. Mandamento de ouro, que nem sempre é executado.

Quarto Mandamento

Você sempre tem de proporcionar alguma medida de valor, real valor, matéria mesmo, com o propósito de validar a informação e todas as outras peças que não têm efetivamente nenhum valor. A decisão de abrir informações efetivamente válidas para suportar as falsas é de responsabilidade do líder e, é claro, deve ser tomado o cuidado de divulgar informações válidas e precisas, porém, o mínimo sensíveis possível.

Quinto Mandamento

O que você quer que seu concorrente faça? Você precisa ter em mãos os recursos, meios, métodos e tudo o mais para determinar o quanto seu rival está seguindo a pista que você quer que ele siga. Não ter idéia do quanto o projeto está funcionando significa alto custo e pouco benefício. Em resumo, você precisa saber o que deverá fazer a partir do instante em que o concorrente esteja fazendo o que você queria que ele fizesse.

Sexto Mandamento

Você tem de ser capaz de seguir o fluxo das informações e as suas pílulas de veneno devem ser cuidadosamente distribuídas para as pessoas certas de modo a alcançar o objetivo.

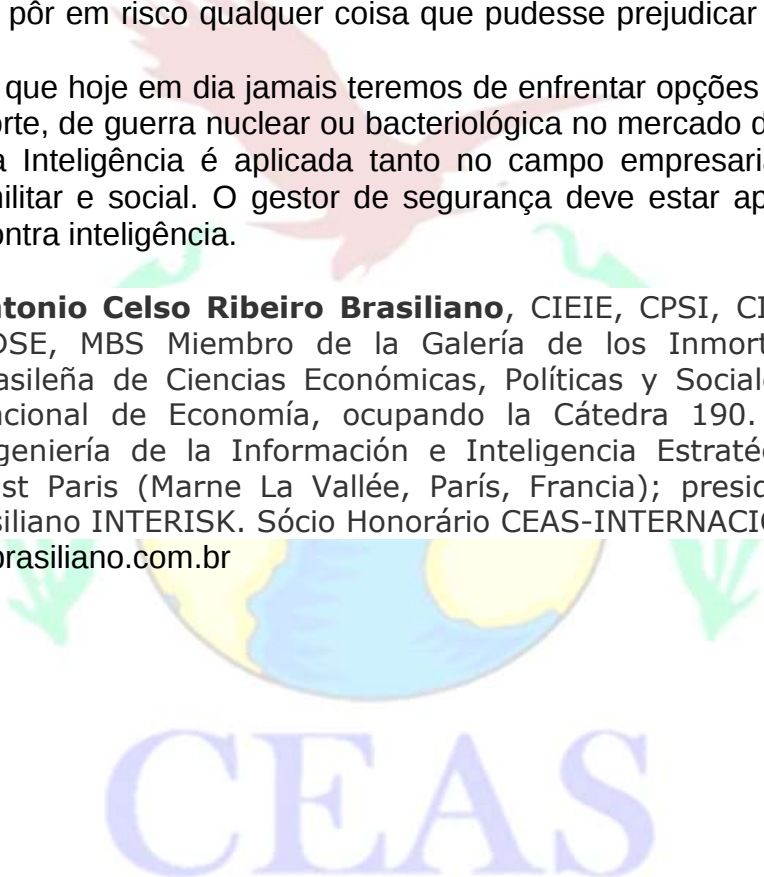
Sétimo Mandamento

A decepção é tipicamente defensiva, você tem de saber proteger suas preciosas fontes de informação. Há momentos em que você tem conhecimento de algo de grande valor, mas não pode usar por causa do comprometimento potencial da fonte. A alternativa para não usar essa informação é seguir a linha de decepção preconizada por Winston Churchill durante a Segunda Guerra Mundial: Em tempo de guerra a verdade é tão preciosa que ela precisa estar sempre rodeada por uma verdadeira corporação de mentiras. Lembre-se do caso em que os Aliados conseguiram acesso à base das máquinas de

criptografia dos alemães. Eles conseguiram uma em 1939 através dos esforços da Espionagem Polonesa; Mais tarde conseguiram um modelo mais recente através de uma operação no Atlântico Norte. Se os alemães tivessem sabido que os seus praticamente indecifráveis códigos estavam sendo normalmente lidos em Bletchley Park, com certeza os teriam mudado. Porém, os Aliados tinham de ser extremamente judiciosos no uso das informações obtidas justamente por isso: não havia nenhum interesse em deixar saber que eles eram capazes de ler as mensagens codificadas. Esse cuidado chegou a extremos, como por exemplo, Churchill deixar bombardear a catedral de Coventry ainda que soubesse que esse seria o alvo principal de um raid aéreo. Se ele tivesse interceptado os bombardeiros alemães, poderia fazer com que os inimigos desconfiassem que suas mensagens operacionais estavam sendo lidas — e decifradas. Churchill preferiu assumir a responsabilidade pelo bombardeio a pôr em risco qualquer coisa que pudesse prejudicar o programa do Dia D.

É claro que hoje em dia jamais teremos de enfrentar opções como essa, de vida ou morte, de guerra nuclear ou bacteriológica no mercado de negócios. Mas a Contra Inteligência é aplicada tanto no campo empresarial como no econômico, militar e social. O gestor de segurança deve estar apto a utilizar técnicas de contra inteligência.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br



CEAS

CISNES NEGROS, QUAL A MELHOR FORMA DE LIDAR COM ESTE TIPO DE RISCO?

É quase impossível prever um evento massivo para os negócios da empresa. Este tipo de evento é denominado de “cisne negro”. Portanto as boas práticas sugerem que em vez de insistir na ilusão de que dá para antever o futuro, os gestores de riscos das corporações deveriam elaborar planos de mitigação, ou seja, redução do impacto de ameaças que fogem à compreensão.

Vivemos no mundo VUCA, extremamente volátil, onde regras rígidas não mais valem para lidar com o dia a dia dos riscos corporativos. O gestor deve estar preparado para tudo. Esse é o nosso maior desafio!

Por exemplo nenhum modelo de projeção vislumbrou o impacto da crise de 2008 que o mundo sofreu, cujas consequências continuam a surpreender economistas e teóricos da gestão. Para piorar, a crise foi agravada, como todos sabemos, pelos chamados modelos de gestão de risco dos bancos — modelos que aumentaram, em vez de limitar, a exposição das instituições ao risco e deixaram o sistema econômico mundial mais frágil do que nunca.

Acontecimentos de baixa probabilidade e alto impacto, praticamente impossíveis de prever — o que chamamos de “cisne negro” —, são cada vez mais comuns. Por causa da internet e da globalização, o mundo virou um sistema complexo, formado de uma trama enredada de relacionamentos e outros fatores interdependentes. Os riscos estão cada vez mais interconectados!

Com a complexidade, surgem não só mais cisnes negros, mas fica impossível prever até acontecimentos ordinários. A única coisa que dá para prever é que a empresa que ignorar cisnes negros vai afundar.

Em vez de tentar antever eventos de baixa probabilidade e alto impacto, devíamos reduzir nossa fragilidade a esse tipo de fenômeno.

Autor de A Lógica do Cisne Negro, Nassim Taleb sugere que administrar o risco é reduzir o impacto daquilo que não entendemos — e não tentar, em vão, criar técnicas sofisticadas e histórias que perpetuem a ilusão de que podemos, sim, entender e prever o ambiente social e econômico.

Nassim enumera pelo menos cinco grandes erros que considera que os gestores de riscos e executivos praticam na tentativa vã de prever o futuro. Escrevi na íntegra o que Nassim Taleb sugere, evitando interpretações. Gostaria que os gestores de riscos fizessem uma reflexão para podermos mudar a forma de encarar os CISNES NEGROS. São eles:

1) Achar que, ao prever eventos extremos, será possível administrar o risco.

É o pior erro que cometemos, por dois motivos. Primeiro porque nossa capacidade de prever cisnes negros é péssima. Segundo porque, ao nos atermos a um punhado de cenários extremos, esquecemos outras possibilidades. No processo, ficamos mais vulneráveis.

Melhor seria pensar nas consequências — ou seja, avaliar o possível impacto de acontecimentos extremos. Cientes disso, empresas energéticas

finalmente deixaram de tentar prever quando poderia haver um acidente numa usina nuclear. O que fazem, agora, é se preparar para a eventualidade. Faça o mesmo. Tente determinar como sua empresa será afetada, na comparação com as concorrentes, por mudanças drásticas no mercado. Uma queda inesperada na demanda ou na oferta, ainda que pequena, abalaria muito a empresa? Se a resposta for sim, ela não suportaria uma queda acentuada em pedidos, um súbito aumento de estoques, e por aí vai.

2) Acreditar que estudar o passado vai nos ajudar a controlar o risco.

O gerente de risco erra ao olhar no retrovisor para enxergar o futuro. Nossa pesquisa mostra que eventos passados não guardam qualquer relação com choques futuros. Não havia precedentes para coisas como a 1ª Guerra Mundial e os ataques de 11 de setembro de 2001. O mesmo vale para o comportamento das bolsas. Até o final da década de 1980, a pior queda [das bolsas americanas] num único pregão tinha sido de cerca de 10%. No dia 19 de outubro de 1987, no entanto, as bolsas caíram 23%. Como explicar que, depois disso, alguém esperasse que qualquer tombo feio fosse se limitar a 23%? A história engana muita gente.

É comum ouvirmos gerentes de risco — sobretudo no setor financeiro — tentarem se justificar com um “Isso não tem precedentes”. O que acham é que, com o devido esforço, é possível encontrar precedente para qualquer coisa e prever tudo. Só que um cisne negro não tem precedente. Para piorar, o mundo de hoje não parece o de ontem; tanto a interdependência quanto a não linearidade são maiores. Certas políticas não provocam efeito nenhum a maior parte do tempo — até que, um dia, causam uma grande reação.

Ninguém leva em conta a aleatoriedade inerente a muitas variáveis econômicas. Uma delas, a aleatoriedade socioeconômica, é menos estruturada e dócil do que a outra, a que encontramos em manuais de estatística e cassinos. Provoca situações de concentração (winner-take-all) com graves consequências. De todas as empresas de capital aberto no mundo, menos de 0,25% responde por cerca de metade do valor total de mercado. De todos os livros publicados, menos de 0,2% gera cerca de metade das vendas. De todos os remédios no mercado, menos de 0,1% responde por pouco mais de metade da receita da indústria farmacêutica. De todos os riscos que corremos, menos de 0,1% causará pelo menos metade do nosso prejuízo.

Por causa da aleatoriedade socioeconômica, não há um fracasso “típico” nem um sucesso “típico”. Há altura e pesos típicos, mas não há uma vitória ou uma tragédia típica. É preciso prever tanto o evento quanto sua magnitude — o que é difícil, pois o impacto em sistemas complexos não é típico.

3) Ignorar conselhos sobre o que não fazer.

Uma recomendação para “não” fazermos algo em geral é mais impactante do que uma sugestão positiva. Aconselhar alguém a não fumar, por exemplo, vale mais do que qualquer outra dica de saúde dada. “Os efeitos nocivos do cigarro são mais ou menos equivalentes aos efeitos positivos somados de toda intervenção médica surgida desde a 2ª Guerra Mundial. Abolir o cigarro traria mais benefícios do que a capacidade de curar o ser humano de todo tipo possível de câncer”, observa o especialista em genética

DruinBurch no livro *Taking the Medicine*. Por essa lógica, se tivessem ouvido o conselho de não se expor excessivamente a eventos de baixa probabilidade e alto impacto, os bancos americanos não ficariam insolventes em 2008 — mas teriam, é claro, ganhado menos lá atrás.

Psicólogos fazem distinção entre o ato comissivo e o omissivo. Embora o impacto seja o mesmo em termos econômicos — o que não é perda, é ganho —, gerentes de risco não tratam as duas coisas igualmente. Dão mais ênfase a registrar lucro do que a evitar prejuízos. Mas uma empresa pode triunfar se evitar perdas enquanto as concorrentes se estrepam — e, isso feito, pode roubar mercado delas. No xadrez, os grandes mestres buscam evitar erros; os novatos tentam vencer. Na mesma veia, o gerente de risco não gosta de não investir e, com isso, conservar valor.

Dar conselho positivo é coisa de charlatão. A seção de negócios nas livrarias está cheia de histórias de sucesso; há muito menos obras sobre o insucesso. Esse menosprezo do conselho negativo faz a empresa tratar a gestão do risco como algo desvinculado da atividade lucrativa, como algo secundário. O que devia fazer é integrar atividades de gestão de risco aos centros de lucro e tratá-los como atividades geradoras de lucro, sobretudo se a empresa estiver sujeita a cisnes negros.

4) Achar que o risco pode ser medido pelo desvio padrão.

O desvio padrão — muito usado na área financeira como indicador do risco de um investimento — não devia ter lugar na gestão de risco. O desvio padrão corresponde à raiz quadrada do quadrado de diferenças médias — não às diferenças médias. O uso de quadrados e da raiz quadrada torna o indicador complicado. Seu único significado é que, num mundo de aleatoriedade controlada, cerca de dois terços da variação deviam ficar dentro de certos limites (os desvios padrão de -1 e $+1$) e que qualquer diferença maior do que sete desvios padrão é praticamente impossível. Mas isso não vale na vida real, onde pode haver oscilações de mais de 10, 20 e às vezes até 30 desvios padrão. O gerente de risco deve evitar usar métodos e indicadores ligados ao desvio padrão, como modelos de regressão, R-quadrado e betas.

Há muita confusão em torno do desvio padrão. Nem analistas quantitativos parecem entender bem o conceito.

5) Não entender que equivalência matemática não significa equivalência psicológica.

Em 1965, em *The Character of Physical Law*, o físico Richard Feynman observou que dois enunciados matematicamente equivalentes podem ser díspares por se apresentarem à mente humana de forma distinta. Na mesma veia, nossa pesquisa mostra que o modo como o risco é formulado influencia a compreensão do mesmo. Se dissermos ao investidor que há chance de que perca todo seu dinheiro somente a cada 30 anos, em média, é mais provável que invista do que se dissermos que a probabilidade de perda de uma certa quantia é de 3,3% ao ano.

O mesmo vale para viagens de avião. Fizemos a seguinte pergunta aos participantes de um experimento: “Você está de férias em outro país e pensa em voar por uma companhia aérea local para visitar uma certa ilha. Segundo

estatísticas de segurança, essa empresa registra, em média, uma queda de avião a cada mil anos. Você dificilmente voltará a essa parte do mundo. Compra a passagem ou não?”. Todos os participantes disseram que sim.

Em seguida, mudamos a segunda frase, que passou a ler: “Segundo estatísticas de segurança, essa empresa registra, em média, uma queda de avião a cada mil voos”. Nos dois casos, a chance de queda é de uma em mil. Só que, no segundo enunciado, o perigo soa maior.

Apresentar o melhor dos cenários normalmente aumenta o apetite pelo risco. Logo, busque sempre outras formas possíveis de apresentação do risco para não se deixar iludir pela formulação ou pela matemática.

Portanto a minha conclusão é que no nosso mundo de hoje, 2017, tudo é uma questão de incentivos. É de desincentivos também. Quem quer ter parte do retorno precisa assumir também parte do risco. Contudo, a própria natureza da remuneração aumenta o risco. Se o bônus que a empresa dá a alguém não puder ser confiscado, esse executivo ou executiva terá um incentivo para ocultar o risco, promovendo para tanto transações com alta probabilidade de gerar pequenos lucros e pequena probabilidade de sérios reveses. Com isso, o executivo garante seu bônus por anos a fio. A empresa perde o executivo ganha!

Além disso, quem administra operações de alto risco, como usinas e bancos, não devia receber bônus, pois é bem provável que busque atalhos para maximizar o lucro.

O risco é muito grande, pois o fator humano superestima a habilidade e subestima o que pode dar errado. Na antiguidade, a húbris(palavra grega que significa que "tudo que passa da medida; descomedimento") era considerada o pior dos defeitos e punida de forma implacável pelos deuses. Basta ver todos os heróis que sofreram retaliação fatal pela megalomania: Aquiles e Agamenon pagaram com a morte pela arrogância; Xerxes foi derrotado devido à presunção ao atacar a Grécia; e muitos generais ao longo da história pereceram por não reconhecer os próprios limites. A empresa que não conhece seu calcanhar-de-aquiles está fadada a sucumbir por causa dele.

Vc conhece o seu? Espero que sim!

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasileiro INTERISK. Sócio Honorário CEAS-INTERNACIONAL.

abrasiliano@brasiliano.com.br

INTERPRETAÇÃO E ANÁLISE DAS INFORMAÇÕES INTEGRADAS EM RISCOS GERA A INTELIGÊNCIA EM RISCOS CORPORATIVOS: POR QUE AS EMPRESAS RELUTAM EM PRATICAR?

Atualmente enfrenta-se grande diversidade de desafios, entre eles as questões tecnológicas. O atual contexto está cada vez mais complexo e dinâmico, pois estamos vivendo a Quarta Revolução Tecnológica. O exemplo disso foi o ataque cibernético que o mundo, incluindo o Brasil, sofreu neste mês de maio de 2017, paralisando inúmeras operações por ter suas informações sequestradas. A sociedade ainda não se deu conta de quebras de paradigmas, alterações de tamanho, velocidade e escopo. O que isto significa em termos de riscos? Um alto grau de análises e interpretações das informações das inúmeras disciplinas de riscos, de forma estruturada e integrada. Por que ainda então as empresas relutam em trabalhar com esta visão?

Adinamicidade 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 para o negócio e, previne contra as incertezas do ambiente de negócios, ajudando desta forma a empresa a priorizar recursos. Faz com que a empresa passe a enxergar na frente, com visão de antecipação.

O grande desafio passa a ser a integração das diversas estruturas de gestão de riscos que as corporações hoje possuem. A integração das disciplinas faz com que o processo de gerenciamento de riscos gere e preserve valor aos acionistas.

Hoje, com a quarta Revolução Industrial em andamento, onde existem três grandes indicadores:

1. Velocidade: a quarta revolução evolui em um ritmo exponencial e profundamente interconectado, com novas tecnologias gerando outras mais novas e mais qualificadas;
2. Amplitude e Profundidade: a quarta revolução industrial possui como base a revolução digital e combina várias tecnologias, levando a mudanças de paradigma sem precedentes da economia, dos negócios, da sociedade e das pessoas.;
3. Impacto Sistêmico: a quarta revolução envolve a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda sociedade.

Vivemos em uma era 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, que no contexto das guerras atuais tornou-se caótico.

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.

O mundo VUCA só pode ser gerenciado com um foco muito grande naquilo que vai gerar resultados e agregar valor para as empresas. Da mesma forma, nós gestores de risco temos que focar nos riscos críticos dentro dos processos que suportam os objetivos estratégicos.

As incertezas passaram a ser a matéria prima dos gestores, e, de forma direta, todos devem saber lidar e gerenciar seus riscos. Daí a importância que as empresas ainda relutam, mas não há como não aceitar, o conceito das Três Linhas de Defesa, onde o dono do processo é o dono do risco. Abaixo o diagrama utilizado como benchmarking de mercado internacional.

Modelo de Três Linhas de Defesa



Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA/FERMA, artigo 41

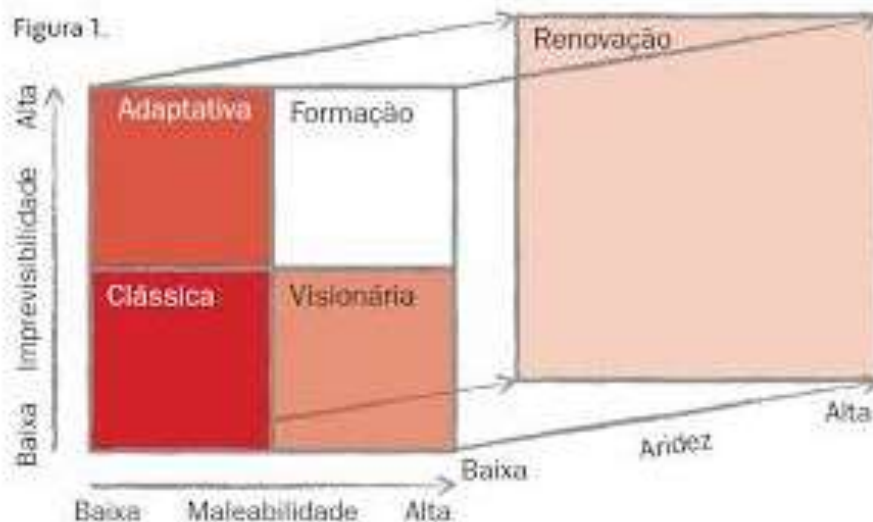
As competências dos gestores de forma geral passou a exigir:

- 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 parado, se ficarmos o inimigo mata! O ótimo é inimigo do bom, conhecem?);
- não ortodoxia, 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 várias abordagens estratégicas ao mesmo tempo, e, com isto, a Gestão de Riscos, tem que possuir uma abordagem holística. A Harvard Business Review Press, nos EUA, lançou o livro *Sua Estratégia precisa de Estratégia*, de Martin Reeves, Knut Haanaes e Janmejaya Sinah, membros de *The Boston Consulting Group* – BCG.

Pela alta dinamicidade em que estamos vivendo, os autores mostram como os enfoques estratégicos se agrupam em cinco categorias, de acordo

com as características do mercado. Ou seja as empresas não mais podem seguir uma única estratégia, mas sim ter na manga uma paleta com as opções, e como camaleão ir mudando de acordo com as condições do mercado. As explicações aprofundadas de cada um destes enfoques oferecem um discernimento crítico para ajudá-lo a encontrar seu enfoque para estratégia para seu ambiente, determinando quando e como executar cada um, e evitando um potencial fatal descasamento. Abaixo uma idéia de estratégia versus as características do mercado.



Dentro deste conceito o Gerenciamento de Riscos Corporativos ganhou corpo e está exigindo dos gestores uma postura mais estratégica. Esta postura estratégica só vai acontecer se, em primeiro lugar a empresa apoiar o conceito das três linhas de defesa, caso contrário o gestor de riscos ficará no operacional, realizando um trabalho que deveria ser dos gestores de linha. Segundo ele tiver condições de ter uma ferramenta de Inteligência em riscos, que consiga integrar as informações e assim ele possa filtrar e interpretar. Por esta razão, é que o departamento deve possuir processo sistêmico e contínuo de análise e interpretação das informações críticas. 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.

Ponto fundamental é que todas as disciplinas de riscos devem estar integradas com um único Framework e com Políticas integradas, visando 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. Abaixo os produtos da Segunda Linha de Defesa, que hoje na grande maioria das empresas não consegue operacionalizar.



A segunda questão é possuir um Sistema que suporte todas estas interações.

Nós da Brasiliano estamos lançando o INTERISK, uma Solução em Inteligência em Riscos, que integra todas as disciplinas e realiza a filtragem das informações estratégicas.



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 ressalta: “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. O gestor deve possuir ferramentas de priorização de processos críticos, fatores de riscos críticos, riscos críticos para elaborar seus planos de ações. Sem isto não há condições de realizar um Gerenciamento Contínuo e com Inteligência.

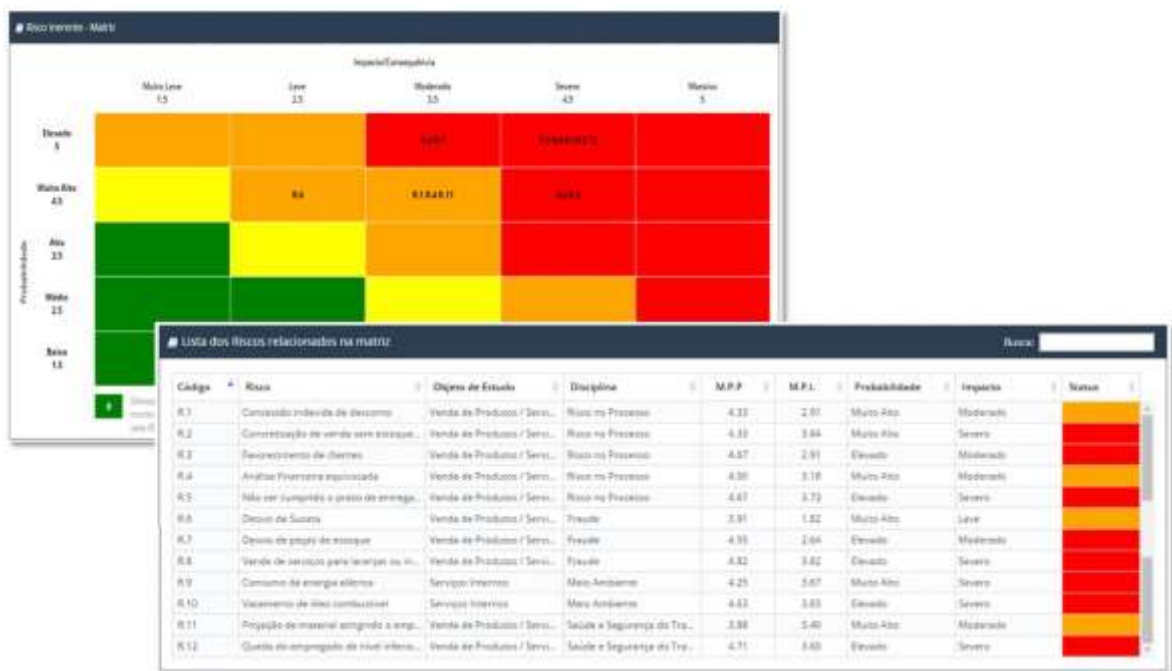


Ferramenta para selecionar processos críticos

INTERISK
Inteligência em Riscos

A Relevância dos fatores de riscos permite ao gestor visualizar quais são as causas motrizes que podem potencializar os riscos.





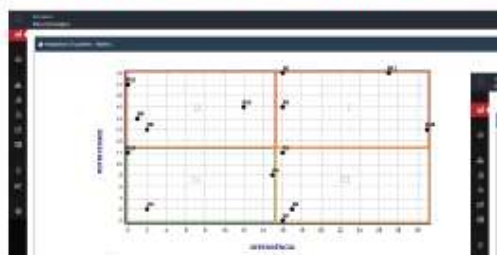
Matriz de Riscos Integrada com todas as disciplinas, onde o gestor pode filtrar os risco de maior relevância.



**Matriz que integra todas as disciplinas,
possibilitando a visão holística**



Matriz de Interconectividade entre Riscos



Matriz de Criticidade



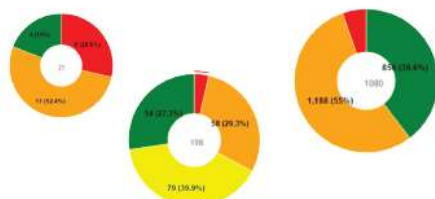
Matriz de Priorização dos Riscos



Por meio da integração da matriz de impactos cruzados com a matriz de riscos residuais é possível analisar a criticidade dos riscos e suas interconectividades, permitindo a priorização dos riscos motrizes de maneira precisa. Assim temos mais clareza nos resultados.

Interconectividade e Criticidade dos riscos, tendo uma Matriz de Priorização.

Painel de controle



Painel com indicadores cruzados permite monitorar a evolução dos riscos e dos planos de ação.

Painel de Controle, para a realização do monitoramento.

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 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 serem 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.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasiliano INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br

CEAS

FUTURO GLOBAL: RISCOS PERMANENTEMENTE CONECTADOS, SÃO GERENCIÁVEIS?

Estamos entrando em um território marcado por turbulências imprevisíveis e mudanças exponenciais para as quais, nós, gestores de riscos, não estão preparados. É uma era em que tudo está sendo reinventado, rediscutido e reprogramado.

O mundo está transformando-se com uma velocidade da luz, na qual os processos organizacionais, as culturas empresariais e os sistemas de tecnologia da informação do século XX, já não suportam às novas demandas deste novo século XXI. As empresas necessitam romper estrategicamente alguns dogmas da administração, impondo um ritmo de muita rapidez, agilidade e criatividade – RAC, suficientes para identificarem e se beneficiarem das janelas de oportunidades. Estas janelas, com aberturas pequenas, abrem e fecham muito rápido, e cabe aos líderes, assessorados pela gestão de riscos, identificarem estes sinais, caso contrário as oportunidades poderão não mais voltarem e a empresa perder o “bonde da história”!

Sabemos que o mundo vive hoje uma expansão exponencial, com uma aceleração muito forte. Os líderes empresariais estão vivenciando em seus processos, serviços e produtos o chamado 6D's: tudo pode ser digitalizado, a venda será no início dissimulada, em seguida irá ser disruptiva, para desmaterializar os serviços e produtos, e como consequência desmonetizar e democratizar.

Qualquer empresa deve estar preparada para acompanhar o ritmo que será definido pelos 6 D's. A única saída estratégica é quebrar os dogmas existentes e, criar algo radicalmente inédito, um verdadeiro inovador modelo de negócio, onde a ousadia e o risco serão os verdadeiros baluarte deste novo século.

O mundo vive a falta de linearidade, ou seja não há mais uma relação direta de causa e efeito, por esta razão o ambiente ficou conhecido com o acrônimo em inglês de VUCA, que significa Volatility, Uncertainty, Complexity e Ambiguity, em português é Volatilidade, Incerteza, Complexidade e Ambiguidade, que chamo de VICA.

O Mundo VICA já foi tema de alguns artigos meus nesta revista, onde descrevi a dificuldade dos líderes e de seus gestores de riscos realizarem uma análise do contexto para a tomada de decisão, em função da alta taxa de volatilidade que leva a uma constante incerteza, fazendo com que as diversas variáveis e riscos acabem se interagindo e interconectando para jogar na frente dos decisores não um único quadro, mas inúmeros quadros do contexto estudado. Qual deles posso ou devo optar? Eis a questão? Algumas empresas foram engolidas pelo VICA pela miopia da sua visão estratégica e a falta de acuidade perceptiva (falta de preparação psicológica e mental para enxergar além do campo de visão e identificar anomalias) de seus líderes.

Lendo o livro de Kevin Kelly, futurista, cofundador da Revista Wired, referência

em tecnologia, chamado de Inevitável, ele prospecta que os objetos serão alimentados pelas informações da mesma maneira que são alimentados pela eletricidade. Kevin tem certeza de que nada será como antes. O futuro está aí e é descrito como o intervalo de tempo que se inicia após o presente e não tem um fim delimitado.

Patrick Dixon, outro futurista, define o futuro através de um acrônimo em inglês: FUTURE – FAST – URBAN – TRIBAL – UNIVERSAL – RADICAL – ETHICAL. Estes são os seis eixos que compõem o futuro:

- 1) Fast – futuro veloz: a velocidade das coisas e a dificuldade de processar essa realidade rápida só tendem a aumentar;
- 2) Urban – futuro urbano: o crescimento desmensurado das cidades do mundo tem alterado o conceito de metrópole para megalópole. As megalópoles serão verdadeiros e autênticos aglomerados de carros, prédios, pessoas, influenciando decisivamente a qualidade de vida de todos;
- 3) Tribal – futuro em tribos: para entender os consumidores há a necessidade de abandonar a segmentação geográfica ou psicográfica e focar nas características tribais. As tribos e os grupos polissociais assumem relevância quando se quer entender o mercado e qual direção devemos seguir.
- 4) Universal – futuro globalizado: a beleza do mundo conectado será aproximar culturas e pessoas, globalizar. Hoje o que acontece em um lugar, outro, em qualquer parte deste planeta é a conectividade permanente!
- 5) Radical – futuro de extremos: o radicalismo positivo é o pensar fora da caixa, ser ousado, arriscar, sonhar, desafiar o “status quo”, conseguir quebrar dogmas e olhar sob outro ângulo e pontos de vistas a realidade atual e o futuro que se aproxima. Fácil? Não! Tem que possuir muita coragem!
- 6) Ethical – futuro ético: é e será o tempero que irá reger o mercado, pois não é mais vale-tudo. Os executivos precisarão serem disruptivos e criativos, mas respeitando as pessoas, o planeta e os agentes de mercado.

Com esta definição simples do futuro, deixa-nos algumas reflexões:

- Estamos prontos para este futuro?
- Estamos preparados para a disrupção?
- Conseguimos fazê-la?
- Conseguimos gerenciar os riscos?

Creio que sim, o futuro acontece para todos, independente de não sabermos quando, nem em que intensidade!!

Vale a pena, estarmos preparados! O futuro é inevitável.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasiliano INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br



RISCOS GLOBAIS 2019 – SUMÁRIO EXECUTIVO DO GLOBAL RISK REPORT

Foi publicado, em janeiro, o relatório do Fórum Mundial, de Riscos Globais 2019. Elaboramos um sumário executivo, responsabilidade do autor, com o objetivo de apontar de forma bem direcionada os pontos relevantes do relatório. Espero que gostem e utilizem.

Introdução

O mundo está paralisado frente a uma possível crise. Os riscos globais estão ficando cada vez mais intensos e conectados, mas a vontade coletiva de enfrentá-los parece estar minguando. Porque? Este é um dos questionamentos estratégicos do relatório.

A resposta é em função da nova fase que os países estão passando em sua questão política, centrada apenas em seu Estado. Esta linha de tendência, segundo o relatório continuou em 2018, traz como consequências questões geopolíticas de “retomar o controle”, sejam elas internas de rivais políticos ou externos de organizações multilaterais ou supranacionais, repercutindo em muitos países e gerando inúmeros problemas.

A energia que os países estão se dedicando com a consolidação dos riscos nacionais enfraquece a disposição de respostas coletivas aos desafios globais emergentes. Portanto o mundo está aprofundando nos problemas globais, sem ter muitas saídas, a não ser que haja mudanças de atitudes. Foram identificadas cinco áreas críticas:

1. vulnerabilidades econômicas;
2. tensões geopolíticas;
3. tensões sociais e políticas;
4. fragilidades ambientais;
5. instabilidades tecnológicas.

Áreas Críticas:

Vulnerabilidades Econômicas

As tensões geoeconômicas aumentaram durante 2018. Os entrevistados estavam preocupados a curto prazo com a deterioração do ambiente econômico internacional, com a grande maioria esperando riscos crescentes em 2019 relacionados a “confrontos econômicos entre grandes potências” (91%) e “erosão de regras e acordos comerciais multilaterais” (88%). A volatilidade do mercado financeiro aumentou em 2018 e os ventos contrários enfrentados pela economia global se intensificaram. A taxa de crescimento global parece ter atingido o pico: as últimas previsões do Fundo Monetário Internacional (FMI) apontam para uma desaceleração gradual nos próximos anos. Isto é principalmente o resultado da evolução das economias avançadas, onde o FMI espera que o crescimento real do PIB desacelere de 2,4% em 2018 para 2,1% em 2019 e 1,5% até 2022. Altos níveis de endividamento global foram uma das vulnerabilidades financeiras específicas

destacadas em 2017 e estas preocupações não diminuíram. A carga total da dívida global é agora significativamente maior do que era antes da crise financeira global, em torno de 225% do PIB mundial. No seu mais recente *Relatório Global de Estabilidade Financeira* o FMI observa que, em países com setores financeiros sistemicamente significativos, a carga da dívida é ainda maior, em 250% do PIB - isso se compara a 210% em 2008. Além disso, um aperto nas condições financeiras globais colocou pressão sobre os países que acumularam dívidas denominadas em dólar, enquanto as taxas de juros estavam baixas. Em outubro do ano passado, mais de 45% dos países de baixa renda estavam em alto risco de sobre endividamento, acima de um terço em 2016.

A desigualdade continua a ser vista como um importante impulsionador do cenário de riscos globais. O aumento da desigualdade de renda e riqueza ficou em quarto lugar na lista de tendências.

Juntamente com a polarização política, a desigualdade corrói o tecido social de um país de maneira economicamente prejudicial: como a coesão e a confiança diminuem, o desempenho econômico provavelmente se seguirá.

O interesse está aumentando em abordagens de economia e finanças que se baseiam na teoria moral e na psicologia social para reconciliar objetivos individuais e comunitários. Por exemplo, mais atenção está sendo dada ao economista e filósofo Adam Smith e ao colocar seu trabalho na “mão invisível” do capitalismo de mercado no contexto de suas ideias sobre obrigação moral e comunidade. Alguns argumentam que muita ênfase foi colocada sobre “os 'desejos' da *Riqueza das Nações*” sobre “os 'desejos' da *Teoria dos Sentimentos Morais*”. Não há remédio fácil: a psicologia moral de diferenças partidárias não é propícia a um compromisso sobre valores, enquanto as divergências geopolíticas discutidas vão complicar qualquer tentativa de encontrar consenso em tentativas ousadas de repensar o capitalismo global. No entanto, esse é o novo desafio!

Tensões Geopolíticas

Em 2018 houve um aumento das tensões geopolíticas entre as principais potências do mundo. Isso ocorre principalmente no campo econômico. O mundo está pessimista: 85% dos entrevistados disseram que esperam que 2019 haverá envolvimento de riscos crescentes de “confrontos políticos entre grandes potências”.

A polarização e a fraca governança levantam sérias questões sobre a saúde política de muitos países.

O relacionamento em desenvolvimento entre a China e os EUA faz parte da paisagem geopolítica emergente descrita no *Relatório de Riscos Globais* do ano passado como “multipolar e multiconceitual”. Em outras palavras, as instabilidades que se desenvolvem refletem não apenas a mudança dos equilíbrios de poder, mas também o fato de que as suposições pós-Guerra Fria - particularmente no Ocidente - de que o mundo convergiria para as normas ocidentais mostraram-se ingenuamente otimistas. As diferenças nas normas fundamentais provavelmente desempenharão um papel importante nos desenvolvimentos geopolíticos nos próximos anos e décadas. Essas diferenças afetarão o panorama de riscos globais de maneiras significativas - desde o

enfraquecimento de alianças de segurança até o enfraquecimento de esforços para proteger os bens comuns globais.

Com o enfraquecimento do multilateralismo e as relações entre as principais potências do mundo em fluxo, o atual cenário geopolítico não é auspicioso para resolver os muitos conflitos prolongados que persistem em todo o mundo. No Afeganistão, por exemplo, as mortes de civis nos primeiros seis meses de 2018 foram as mais altas em 10 anos, segundo a ONU, enquanto a parcela dos distritos controlados pelo governo afegão, apoiado pelos Estados Unidos caiu de 72% em 2015 para 56% em 2018. Na Síria, vários estados estão agora envolvidos em um conflito civil no qual centenas de milhares morreram. E no Iêmen, as baixas diretas da guerra são estimadas em 10.000 e até 13 milhões de pessoas correm o risco de morrer de fome, como resultado de interrupções na alimentação e outros suprimentos, de acordo com um alerta da ONU em outubro de 2018.

Um desenvolvimento geopolítico positivo desde a última edição deste relatório foi o abrandamento das tensões e volatilidade relacionadas ao programa nuclear da Coreia do Norte, após o aumento da diplomacia envolvendo os Estados Unidos, Coreia do Sul e Coreia do Norte. Isso pode ter influenciado uma queda acentuada - de 79% para 44% - na proporção dos entrevistados que esperam que o risco de “conflito ou incursão militar entre Estados” aumente no próximo ano. No entanto, pelo terceiro ano consecutivo, as armas de destruição em massa foram classificadas como o risco global número um em termos de impacto potencial.

Tensões Sociais e Políticas

Em todo o mundo, as instabilidades geopolíticas crescentes são correspondidas - e frequentemente exacerbadas - por contínuas pressões políticas internas. A crescente polarização das sociedades perdem apenas para a mudança climática como um motivador subjacente dos desenvolvimentos no cenário de riscos globais. Muitas democracias ocidentais ainda estão lutando com padrões de fragmentação política e polarização pós- crise que complicaram o processo de fornecer governança estável e eficaz. Mas esta é uma questão global, não apenas um “problema do primeiro mundo”.

A polarização e a fraca governança levantam sérias questões sobre a saúde política de vários países. Em muitos casos, as diferenças partidárias são mais profundas do que há muito tempo. Um círculo vicioso pode se desenvolver, no qual a diminuição da coesão social coloca uma pressão cada vez maior sobre as instituições políticas, minando sua capacidade de antecipar ou responder aos desafios da sociedade.

Este problema é ainda mais agudo quando os desafios globais exigem cooperação ou integração multilateral: níveis mais fracos de legitimidade e responsabilização provocam uma reação antielitista. O mesmo acontece com as falhas da política multilateral e do desenho institucional. Por exemplo, agora é amplamente reconhecido que mais deveria ter sido feito para fornecer proteção ou remédios aos perdedores da globalização.

Fragilidades Ambientais

Os riscos relacionados ao meio ambiente dominam o Relatório de Riscos Globais pelo terceiro ano consecutivo, representando três dos cinco principais riscos por probabilidade e quatro por impacto. O clima extremo está novamente por conta própria no quadrante superior direito (alta probabilidade e alto impacto).

O ano de 2018 foi outro de tempestades, incêndios e inundações. De todos os riscos, é em relação ao ambiente que o mundo está mais claramente cambaleando frente às catástrofes. O Painel Intergovernamental sobre Mudanças Climáticas (IPCC) disse em outubro de 2018 que temos no máximo 12 anos para fazer as mudanças drásticas e sem precedentes necessárias para evitar que as temperaturas globais médias subam além da meta de 1,5°C do Acordo de Paris.

Nos Estados Unidos, a Quarta Avaliação do Clima Nacional alertou em novembro que sem reduções significativas nas emissões, as temperaturas globais médias poderiam subir 5°C até o final do século.

A interconexão de risco de falha de mitigação e adaptação às mudanças climáticas com a materialização de eventos climáticos extremos. O ritmo acelerado da perda de biodiversidade é uma preocupação especial. A mudança climática está exacerbando a perda de biodiversidade e a causalidade vai nos dois sentidos: muitos ecossistemas afetados - como oceanos e florestas - são importantes para absorver as emissões de carbono. Ecossistemas cada vez mais frágeis também apresentam riscos à estabilidade social e econômica. Por exemplo, 200 milhões de pessoas dependem dos ecossistemas costeiros de manguezais para proteger seus meios de subsistência e segurança alimentar contra tempestades e elevação do nível do mar. Uma estimativa do valor econômico nacional dos “serviços ecossistêmicos” - benefícios para os seres humanos, como água potável, polinização ou proteção contra inundações - o coloca em US\$ 125 trilhões por ano, cerca de dois terços acima do PIB mundial.

Na cadeia alimentar humana, a perda de biodiversidade afeta a saúde e o desenvolvimento socioeconômico, com implicações para o bem-estar, a produtividade e até mesmo a segurança regional. A desnutrição de micronutrientes afeta até 2 bilhões de pessoas. É tipicamente causado pela falta de acesso a alimentos de variedade e qualidade suficientes. Quase metade das calorias vegetais do mundo é fornecida por apenas três culturas: arroz, trigo e milho. A mudança climática agrava os riscos. Em 2017, os desastres relacionados ao clima causaram uma aguda insegurança alimentar para aproximadamente 39 milhões de pessoas em 23 países. Menos obviamente, níveis aumentados de dióxido de carbono na atmosfera estão afetando a composição nutricional de alimentos básicos, como arroz e trigo. Pesquisas sugerem que até 2050 isso poderia levar a deficiências de zinco para 175 milhões de pessoas, deficiências de proteína para 122 milhões e perda de ferro na dieta para 1 bilhão.

Como os riscos ambientais se cristalizam com frequência e severidade crescentes, o impacto nas cadeias globais de valor provavelmente se intensificará, enfraquecendo a resiliência geral. As interrupções na produção e entrega de bens e serviços devido a desastres ambientais aumentaram em 29% desde 2012. A América do Norte foi a região mais afetada por interrupções na cadeia de fornecimento relacionadas ao meio ambiente em 2017; Essas interrupções foram devidas principalmente a furacões e incêndios florestais.

Por exemplo, na indústria automotiva dos EUA, apenas incêndios em fábricas e fusões de empresas causaram mais interrupções na cadeia de suprimentos do que furacões. Quando as interrupções são medidas pelo número de fornecedores afetados, e não pelo número de eventos individuais, os quatro gatilhos mais significativos em 2017 foram furacões, condições meteorológicas extremas, terremotos e inundações. Os transtornos na cadeia global de fornecimento e reciclagem de resíduos durante o ano de 2018 podem ser um antegosto. A China proibiu a importação de resíduos estrangeiros, incluindo quase 9 milhões de toneladas de sucata de plástico, para reduzir a poluição e sobrecarregar seus sistemas ambientais nacionais. Essa proibição expôs fraquezas na capacidade de reciclagem doméstica de muitos países ocidentais. Resíduos plásticos construídos no Reino Unido, Canadá e vários estados europeus. No primeiro semestre de 2018, os Estados Unidos enviaram 30% do plástico que teria ido anteriormente para a China em aterro, e o resto para outros países, incluindo Tailândia, Malásia e Vietnã. No entanto, todos esses três países já anunciaram suas próprias novas restrições ou proibições de importações de plástico. Em suma, à medida que o impacto dos riscos ambientais aumenta, será cada vez mais difícil tratar esses riscos como externalidades que podem ser ignoradas ou remetidas. Será necessária uma ação internacional e nacional, coordenadas para internalizar e mitigar o impacto da atividade humana nos sistemas naturais.

Instabilidade Tecnológica

A tecnologia continua desempenhando um papel importante na formação do panorama de riscos globais para indivíduos, governos e empresas. Fraude e roubo maciços de dados foi classificado como risco global número quatro por um horizonte de 10 anos, com “cyber-ataques” no número cinco. Isso mantém um padrão registrado no ano passado, com os riscos cibernéticos consolidando sua posição ao lado dos riscos ambientais no quadrante de alto impacto e alta probabilidade do Panorama de Riscos Globais. A grande maioria dos entrevistados esperava aumentar os riscos em 2019 dos ataques cibernéticos, levando ao roubo de dinheiro e dados (82%) e interrupção das operações (80%).

A pesquisa reflete como novas instabilidades estão sendo causadas pelo aprofundamento da integração de tecnologias digitais em todos os aspectos da vida. Cerca de dois terços dos entrevistados esperam que os riscos associados a notícias falsas e roubo de identidade aumentem em 2019, enquanto três quintos disseram o mesmo sobre a perda de privacidade para empresas e governos.

Ataques cibernéticos maliciosos e protocolos de segurança cibernética novamente levaram a violações maciças de informações pessoais em 2018. O maior foi na Índia, onde o banco de dados de identificação do governo, Aadhaar, supostamente sofreu várias violações que potencialmente comprometeram os registros de todos os 1,1 bilhões de cidadãos registrados. Foi relatado em janeiro que os criminosos estavam vendendo acesso ao banco de dados a uma taxa de 500 rúpias por 10 minutos, enquanto em março um vazamento em uma empresa estatal permitia que qualquer pessoa baixasse nomes e números de identificação.

Por outro lado, as violações de dados pessoais afetados, cerca de 150 milhões de usuários da aplicação MyFitnessPal, e cerca de 50 milhões de usuários do Facebook.

As vulnerabilidades cibernéticas podem vir de direções inesperadas, como mostrado em 2018 pelas ameaças Meltdown e Spectre, que envolviam fraquezas no hardware do computador, e não no software. Eles afetaram potencialmente todos os processadores Intel produzidos nos últimos 10 anos. No ano passado, também houve evidências contínuas de que os ataques cibernéticos representam riscos para a infraestrutura crítica. Em julho, o governo dos EUA afirmou que hackers tinham acesso às salas de controle de empresas de serviços públicos dos EUA.

A potencial vulnerabilidade da infraestrutura tecnológica crítica tornou-se cada vez mais uma preocupação de segurança nacional. A segunda interconexão de risco mais citada foi o emparelhamento de ataques cibernéticos com uma falha crítica na infraestrutura de informações.

Aprendizado de máquina ou inteligência artificial (IA) está se tornando mais sofisticado, com potencial crescente para ampliar os riscos existentes ou criar novos, particularmente quando a Internet das Coisas conecta bilhões de dispositivos. Inovações semelhantes podem ocorrer em outros campos. Por exemplo, o potencial de agentes maliciosos na biologia sintética usarem a inteligência artificial para criar novos patógenos, tal como “computação afetiva” - referindo-se à Inteligência Artificial que pode reconhecer, responder e manipular as emoções humanas.

Entre os impactos mais difundidos e disruptivos da Inteligência Artificial nos últimos anos tem sido o seu papel nosurgimentodecâmarasdeecodamídiadenotíciasfalsas, umriscoque69%dosentre vistadosesperam aumentar em 2019. Uma possível razão citada pelos pesquisadores é que notícias falsas tendem a evocar emoções fortes: “tweets falsos tendem a provocar palavras associadas a surpresa e desgosto, enquanto tweets precisos invocam palavras associadas à tristeza e à confiança”. A interação entre emoções e tecnologia é provável para se tornar uma força cada vez mais disruptiva.

Prof. Dr. Antonio Celso Ribeiro Brasileiro, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS Miembro de la Galería de los Inmortales de la Academia Brasileña de Ciencias Económicas, Políticas y Sociales - ANE - Academia Nacional de Economía, ocupando la Cátedra 190. Doctor en Ciencia e Ingeniería de la Información e Inteligencia Estratégica por la Université East Paris (Marne La Vallée, París, Francia); presidente de la empresa Brasiliano INTERISK. Sócio Honorário CEAS-INTERNACIONAL.
abrasiliano@brasiliano.com.br