



## RISCO DE COMPLIANCE

**EM FOCO**

Política de Gestão de Risco: o documento basilar

**ANÁLISE**

Responsabilidades sobre a Conexão Wireless

## Ponto de Vista

### Editorial

### Em Foco

- Políticas de Gestão de Risco.....7
- A importância do Compliance nas organizações .....13

### B&A Entrevista

- Destrinchando a Perícia Eletrônica – Parte 2 .....19

### Acontece na Brasiliano .....27

### Segurança da Informação

- FATO, métricas não quantificam o risco da informação .....31

### Análise

- Responsabilidades sobre a conexão Wireless .....35

### Treinamento

- Método no Ensino Especializado.....38

### Ler&Saber



A revista Gestão de Riscos é uma publicação eletrônica mensal da Sicurezza Editora.  
Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL

**Diretores** | Antonio Celso Ribeiro Brasiliano e Enza Cirelli. **Edição e Revisão** | Mariana Fernandez. **Arte e Diagramação** | BM Design

**Colunistas** | Álvaro Takei e Mariana Fernandez. **Colaboradores desta edição** | Andre Pitkowski, Camilla do Vale Jimene e Renato Opice Blum

**Brasiliano & Associados Online** | [www.brasiliano.com.br](http://www.brasiliano.com.br) **Blog da Brasiliano & Associados** | [www.brasiliano.com.br/blog](http://www.brasiliano.com.br/blog)

# A MIOPIA ÉTICA

Como é possível uma sociedade enganar-se a si própria? Como podemos mentir para nós mesmos e acreditar na mentira ou remar de costas rumo a um objetivo?

Qual o lugar, o valor e a interligação dos projetos, desejos e aspirações de cada pessoa em particular – ética pessoal – no contexto da convivência em sociedade – ética cívica?

“Todas as grandes tentativas são arriscadas, e é verdadeiro o provérbio segundo o qual aquilo que vale a pena nunca é fácil!” (Platão em a República).

Estamos vivenciando, hoje, na nossa sociedade (não só na sociedade brasileira, mas como sou brasileiro, tenho que falar dela, pois é nela que vivo e sobrevivo), de uma forma direta, a queda dos valores morais. Essa queda é resultado de dois conflitos: o interpessoal (disputa entre nós e eles) e o intrapessoal (nós agora e nós depois – futuro). O conflito intrapessoal envolve o exercício contínuo de uma autoridade interna, que pode afetar a noção do valor no tempo, fazendo com que a parcialidade moral impacte a percepção que as pessoas tem de si e a sua interação com as demais.

Entram nesse contexto as decisões de longo prazo – estratégicas – como as de curto prazo – táticas. As duas são tomadas no presente, mas com horizontes diferentes. As estratégicas visam a realização de objetivos mais estruturados e permanentes, enquanto as táticas são objetivos e resultados imediatos, podendo ser, dependendo da decisão, meras ações sem valor para o futuro.

Escrevo isso porque, hoje, as fraudes nas empresas crescem em proporções geométricas, e quando digo fraude, estou me referindo ao sentido amplo da palavra. Fraude como conceito de burlar não só as regras empresariais, o código de conduta, mas sob o ponto de vista moral e ético.

As pessoas formam a empresa, a sociedade empresarial, e, por isso, não podem estar movidas só pela satisfação imediata, mesmo sabendo que suas ações são contraproducentes no longo prazo. Chamo isso de MIOPIA ÉTICA, pois leva à traição dos valores morais. A parcialidade moral, ou seja, quando as pessoas legislam em causa própria possui como resultado direto o auto-engano.

O Secretário de Segurança Pública do Estado do Rio de Janeiro, o delegado Federal José Mariano Beltrame, em entrevista a revista Veja em 2007 (edição 2032 de 31 de outubro de 2007) afirmou que não existe mais crime famélico, o que quer dizer que ninguém mais pratica o delito por pura necessidade, mas sim para e pela estrutura criminosa hoje existente na cidade do Rio de Janeiro. Afirma também que a sociedade carioca é conivente pelo status quo vigente. Ou seja, a atitude das pessoas colabora para a manutenção do ciclo vicioso. Indo desde o pagamento de uma “cervejinha” ao policial para escapar da multa de trânsito, até pagamentos para as “comunidades” (entende-se facções criminosas), com o objetivo de realizar distribuição de seus produtos com tranquilidade, e a sonegação de impostos. Beltrame afirma ainda que no Brasil, e no Rio de Janeiro em particular, a convivência promíscua entre o legal e o ilegal, o formal e o informal, provoca a manutenção ambígua do status quo da cidade do Rio de Janeiro.

Tenho que concordar em gênero número e grau: a sociedade possui uma visão de curto prazo. As pessoas legislam em causa própria sim, não querendo enxergar as co-responsabilidades.

Não assumem a parcela de responsabilidade, tanto a pessoa como a empresa. O problema da miopia ética pode ser retratado de forma magnífica pela tradição poética grega em torno dos perigos enfrentados pelos navegantes ao ouvir o canto das sereias. Doce caminho, amargo fim!!! A literatura grega registra duas soluções vitoriosas. Uma delas foi a saída encontrada, no calor da hora tendo Orfeu, o incomparável gênio da música e da poesia na mitologia grega. Conseguiu tocar uma música mais doce e sublime que o canto das sereias. Evitou assim que seu navio fosse atraído. A outra solução foi a encontrada por Ulisses, o herói da Odisséia. Para evitar ser atraído pelo canto das sereias, fez com que seus homens tapassem os ouvidos com cera, menos o dele, pois ele queria ouvir e sentir a atração. Exigiu que o prendessem ao mastro e que ignorassem suas ordens. Essa medida também evitou que seu navio fosse atraído.

Lição para seus executivos: Ulisses estava ciente de que não resistiria. Saber não basta!! O que salvou Ulisses não foi a consciência da falsidade moral, mas a sabedoria de não superestimar em momento algum a sua capacidade de resistência ao poder de sedução das sereias. Atando-se ao mastro do navio, ele abriu temporariamente mão de sua liberdade de escolha no presente para salvar a sua vida e liberdade futuras.

Os mares empresariais estão infestados de “sereias”. Alguns destes cantos podem ser: “vamos economizar, aumentar nossas margens, sonegando impostos, abrindo empresas intermediárias”; “vamos cumprir metas financeiras, fazendo caixa, mudando prazos de pagamentos, não importando com os fornecedores e parceiros”; “vamos pagar para a polícia fazer nossa proteção e nossa investigação”; “vamos fazer acordos com a comunidade para poder entregar nossos produtos”; “vamos pagar cervejinha aos guardas para que nossa frota possa circular”; e muitos outros que conhecemos e que a grande maioria ainda pratica!!!!!!!

Qual seria então o mastro a que devemos nos amarrar?? A única segurança duradoura é o comprometimento com a responsabilidade, a franqueza, o respeito e a integridade. Quando não estamos seduzidos e atraídos, sabemos que esses valores são a chave para o sucesso e auto-estima. Por isso, é fundamental que os executivos de forma geral “prendam-se ao mastro” da ética.

Somente seguindo, e, mais importante, acreditando na ética é que poderemos dar exemplo e guiar nossas equipes até um porto seguro. As regras impessoais da ética cívica são necessárias. Elas existem não para nos salvar, mas para nos proteger uns dos outros e de nós mesmos.

Eduardo Giannetti escreveu na últimas páginas de seu livro o Auto-Engano: “ O grande desafio é encontrar o equilíbrio entre as exigências da ética cívica e as demandas da ética pessoal [...] Os riscos e as ameaças, como sempre, estão nos excessos de ambos os lados [...] A passagem é estreita. Nenhuma solução é definitiva. Toda vitória é parcial, cada avanço traz novos desafios e qualquer conquista é passível de retrocesso. A prevenção do mal ajuda, mas não sacia o desejo humano de encontrar o bem. Navegar é preciso. Ouvidos bem abertos, olho na bússola, mastro à mão.”

*“Cada homem faz seu próprio naufrágio”*

*Lucano (poeta romano do século I DC)*

Boas leitura e sorte!!!

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

sua EMPRESA possui TÉCNICAS ?  
para GERENCIAR riscos

Ou simplesmente salta  
para o infinito...

Para sua empresa ser **COMPETITIVA**, possuir **FLEXIBILIDADE** e **AGILIDADE**, há necessidade de compreender a dinâmica dos seus riscos corporativos. A **Brasiliano&Associados** ajuda você através de metodologia interativa, identificar, analisar e tratar os riscos e os seus fatores facilitadores. Propõe soluções integradas, com uma visão holística do contexto, otimizando recursos na mitigação e gerenciamento de riscos.

 **b&a**  
BRASILIANO & ASSOCIADOS

informações | [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)

## MUITO ALÉM DO “C”

O que o descumprimento de leis, regulamentações, códigos de conduta e boas práticas podem acarretar nas organizações? O risco legal, de sanções regulatórias, de perda financeira ou de reputação é a maior fatia do artigo de Antonio Celso Ribeiro Brasileiro.

Mas qual é o maior risco do Compliance, o C do GRC (Governança, Risco, Compliance).

O tema é explanado sucintamente nesta edição da Gestão de Riscos. Governança, auditoria, ética e risco são relacionados à prática, completando o tema de forma maestral.

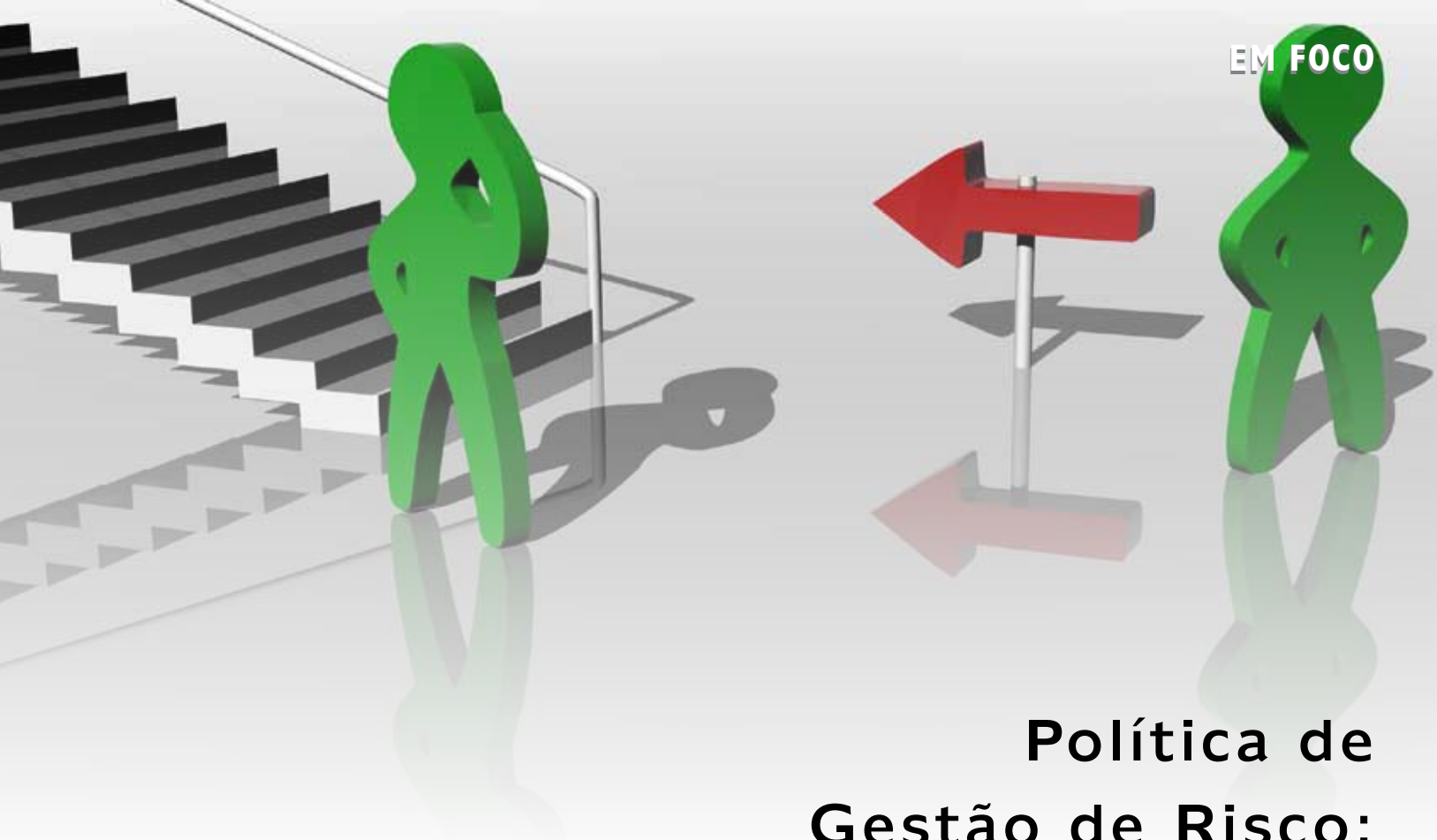
Nesta edição você irá conferir:

- Política de Gestão de Risco é fundamental! Num artigo completo sobre o tema, você saberá o que deve ter o documento que conterá as diretrizes na gestão de risco da sua organização.
- Camilla do Vale Jimene e Renato Opice Blum trazem um artigo que aborda as Responsabilidades sobre a Conexão Wireless sob o ponto de vista jurídico, mostrando a necessidade de proteção das conexões sem fio para que o usuário não sofra sanções penais.
- A importância do Método no Ensino Especializado é na coluna Treinamento, de Álvaro Takei.
- Andre Pitkowski mostrará em seu artigo de segurança da informação, onde é recomendado o uso de métricas para bloquear e combater os riscos antes de implementar criteriosos modelos de Gestão de Riscos.
- Todos os feitos recentes da Brasileiro & Associados no sul e sudeste do país, na coluna Acontece.
- A continuação da entrevista exclusiva com o Presidente do Instituto Brasileiro de Peritos Giuliano Giova, trazendo dicas e esclarecimentos para candidatos à área e interessados em segurança eletrônica.
- Lançamentos saídos da prensa da Sicurezza Editora: o novo Método Brasileiro e as Formas do Crime de Tulio Kahn.

Necessidades latentes de conhecimento preenchem o conteúdo da Gestão de Riscos deste mês, eclética no que tange ao risco, educadora, sem blá, blá, blá.

Boa leitura!

Mariana Fernandez  
Editora



# Política de Gestão de Risco: o documento basilar

*Mariana Fernandez*

O termo política é derivado do grego antigo πολιτεία (politeía), que indicava todos os procedimentos relativos à pólis, ou cidade-Estado.

Filosoficamente, política é “o conjunto dos meios que permitem alcançar os efeitos desejados”, para Russel, os “meios adequados à obtenção de qualquer vantagem”, segundo Hobbes ou ou “a arte de conquistar, manter e exercer o poder, o governo”, que é a noção dada por Nicolau Maquiavel, em O Príncipe.

Política pode ser ainda a orientação ou a atitude de uma empresa em relação a certos assuntos e problemas de seu interesse: política financeira, política de qualidade, política de gestão de riscos.

## **A POLÍTICA DE GR NAS ORGANIZAÇÕES**

Cumprindo seu compromisso com a sociedade, acionistas, colaboradores diretos e indiretos, as empresas devem posicionar seu gerenciamento de riscos como um desafio indispensável para as operações do negócio bem como para manter e melhorar seu valor corporativo.

Em nenhum tipo, tamanho ou segmento de organização a gestão de riscos é algo dispensável. Em qualquer empresa, seu gestor deve estar atuando na gerência de seus riscos.

Segundo o especialista em Gestão de Riscos, Antonio Celso Ribeiro Brasileiro, mesmo que comece por áreas específicas, “em princípio a gestão de riscos tem que ser implantada na empresa como um todo”, ou seja, tem que permear a empresa por inteiro.

Essa premissa se deve à concepção de que a gestão de riscos é um processo que deve ser executado com a mesma preocupação com que se prima pela qualidade. Brasileiro destaca a comparação justificando a busca pela qualidade “desde empresas pequenas até grandes corporações” pois “a filosofia é a mesma”.

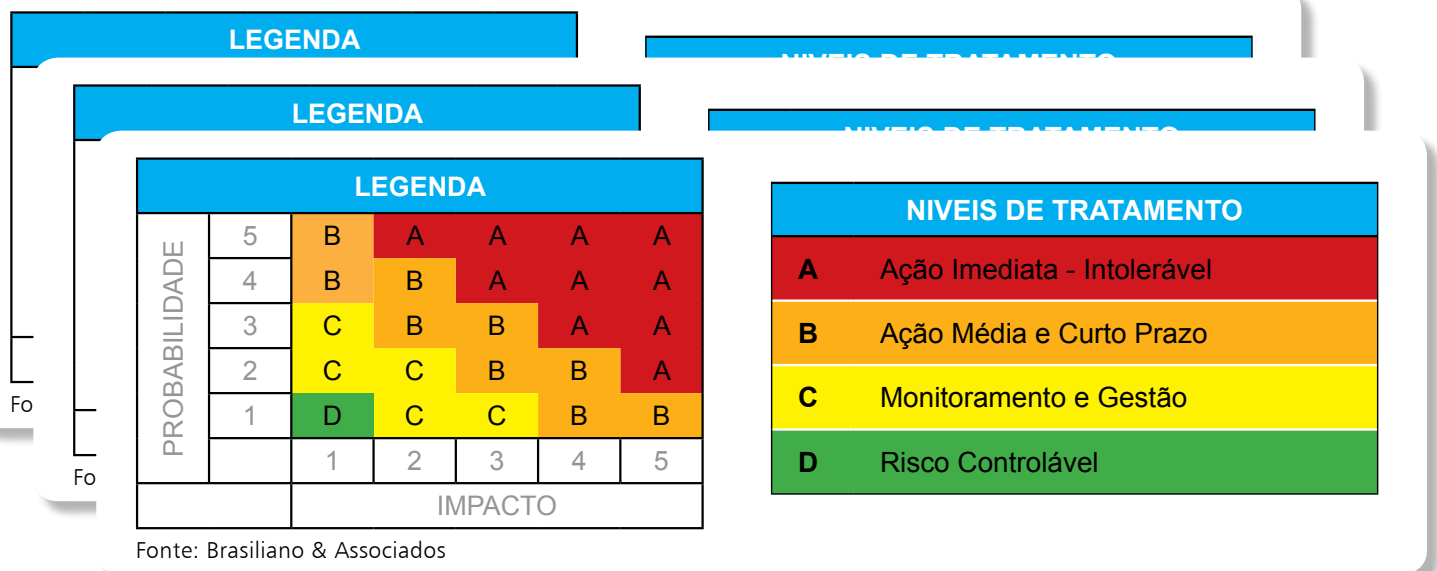
Portanto, não há como gerir os riscos apenas de áreas específicas ou em projetos isolados da empresa.

O estabelecimento de uma política de gestão de riscos deve ser norma de conduta de qualquer organização. Por que? Porque

a política é uma diretriz onde a empresa (acionistas, stakeholders, conselho de administração, proprietários) vai estabelecer seu processo de gestão de risco, a metodologia eleita, ou seja, quais serão os critérios para se estabelecer os níveis de criticidade, seguindo os preceitos da norma de gestão de riscos ISO 31000 que pede a citação da política, procedimento e metodologia.

Segundo Brasileiro, é importante estabelecer na política de gestão de riscos o apetite ao risco da empresa, que é a definição do nível de risco que a organização está disposta a assumir, para se saber quanto se poderá arriscar “tanto positivamente quanto negativamente.”

Balizar as decisões e procedimentos dos colaboradores, é para isso que serve a PGR. Seguindo as normas contidas na política de gestão de riscos da empresa, na utilização de determinada ferramenta, Brasileiro exemplifica que “se o risco cair no quadrante vermelho por exemplo, ele (gestor) sabe que ele tem que tratar, porque ele não pode simplesmente deixar o risco naquele quadrante porque é política da empresa que não tenha risco no quadrante vermelho”.





Segundo texto da norma AS/NZS 4360:2004, a norma de gestão de riscos sobre a qual se baseou a ISO 31000, “a política é um documento sucinto, de nível superior, que aprova uma abordagem para a gestão de riscos e também cria as ligações com outras estratégias da empresa. Ela deve ser incorporada às demais políticas de gestão da organização.”

A função do documento é ser um balizador de conduta e procedimento e apoio à decisão. Por isso a importância de ser um documento formal, que possa ser implementado, elaborado, que vá para a alta gestão da empresa onde é assinado e depois propagado para todos os stakeholders para que esses assumam conscientemente as diretrizes da gestão de risco da corporação.

## **POLÍTICA E FILOSOFIA ANDAM JUNTAS**

A política de gestão de riscos deve ser integrada à filosofia de gestão da organização porque é um documento que tem que estar alinhado com os objetivos estratégicos da empresa, e não antagônico, contraditório. Para isso é necessário que se respeite a estrutura da organização, que se esteja de acordo com seu pensamento e com o perfil de seus colaboradores.

Pode-se conceber uma estrutura de gestão de riscos descentralizada ou centralizada, ou pode-se mesmo implantar um autocontrole. Há diversas formas de se fazer uma gestão, e é na política que devem estar escritas essas formas escolhidas.

Por isso é importante que a política de Gestão de Riscos esteja alinhada com as outras políticas... de RH, financeira e por aí afora.

A PGR deve, primeiramente, estar alinhada ao objetivo estratégico da empresa.

Em segundo lugar, deve seguir as boas práticas de mercado.

Hoje, segundo Brasileiro, “tem que se estar alinhado à norma ISO 31000, não tem muito como fugir disso... o processo como um todo[...] mas o alinhamento maior deve ser com os objetivos estratégicos da empresa.”

## **QUEM DEVE ELABORAR?**

Teoricamente falando seria o gestor de riscos. “Mas como ainda muitas empresas não têm gestor de riscos, isso virou uma verdadeira ‘salada russa’”, diz Brasileiro.

Uma linha de conduta de muitas empresas é a criação da política por uma equipe de auditoria, que fornece-a para a empresa e depois a audita.

Outra linha é a criação da política pelo pessoal da área administrativa, ou da área de controladoria, ou da área de compliance.

“Hoje não tem uma fórmula de bolo, mas, basicamente, teria que ser um departamento, que é o de gestão de riscos, que teria como missão elaborar sua própria e depois disseminá-la”, esclarece o especialista.



## O QUE DEVE CONTER?

Segundo Brasileiro “todas as informações, não pode esconder nada”, isso porque a política de gestão de riscos não é um documento confidencial. Alí se dirá, como forma de governança corporativa, como a empresa fará a gestão de seus riscos.

Dessa forma, as empresas têm que expor sua PGR de forma totalmente transparente, pois, quanto mais transparente for, melhor será a assimilação por parte dos colaboradores, ou seja, as diretrizes irão ganhar uma capilaridade muito grande.

“É errado a empresa tratar esse documento como sigiloso. Isso não existe! Tem que ser aberto para que o público saiba qual é a tecnologia”, acrescenta o especialista.

Uma das grandes formas de se implantar a PGR é através de workshops. Após a publicação e distribuição do documento, fazem-se palestras, workshops, para que o público interno tome conhecimento da política.

Empresas que possuem ções na bolsa de valores, por exemplo, fazem isso através de seus relatórios de governança corporativa: listam seus riscos, mostram a matriz de riscos. É outra forma de mostrar-se transparente e ganhar a confiança dos stakeholders, uma medida de governança.

Alguns exemplos de informações que podem ser incluídas na política de uma organização, segundo a norma AS/NZS 4360:2004, são:

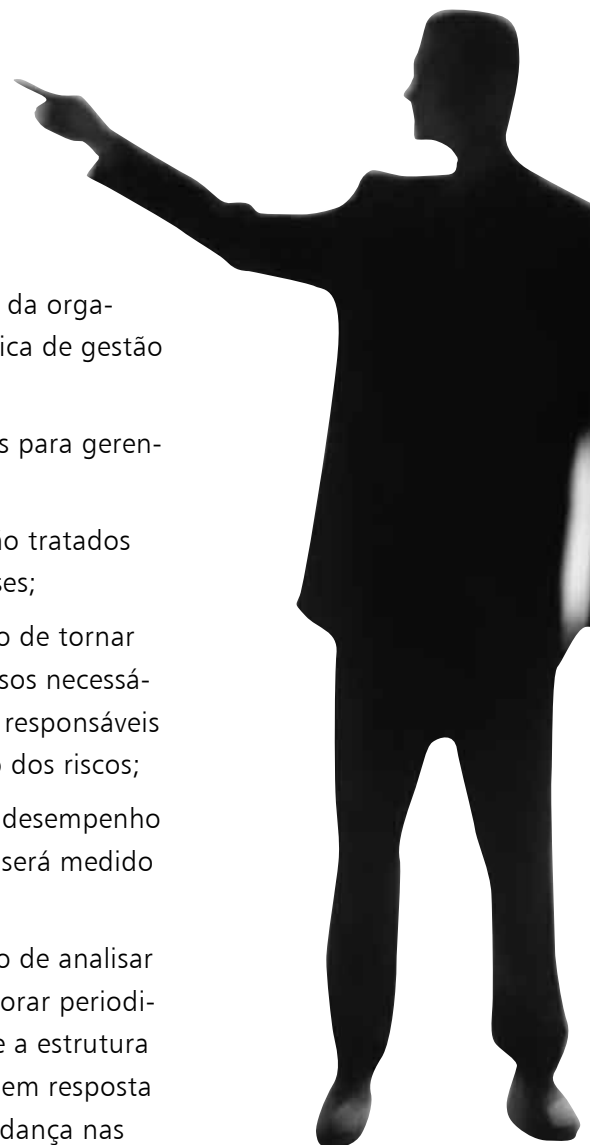
- os objetivos e a base para o gerenciamento dos riscos;
- as relações entre a política e os planos estratégico e operacional da organização;
- a extensão ou gama de riscos que precisam ser gerenciados;
- diretrizes sobre o que deve ser considerado risco aceitável;

- quem são os responsáveis pelo gerenciamento dos riscos;
- o suporte e conhecimento disponíveis para auxiliar os responsáveis pelo gerenciamento dos riscos;
- o nível de documentação requerido; e
- os requisitos para monitorar e analisar criticamente o desempenho organizacional em relação à política.

De acordo com a nova norma da gestão de riscos no mundo *ISO 31000: Principles and Guidelines for Risk Management*, a gestão de riscos deve estabelecer “claramente os objetivos e o comprometimento da organização em relação à gestão de riscos”.

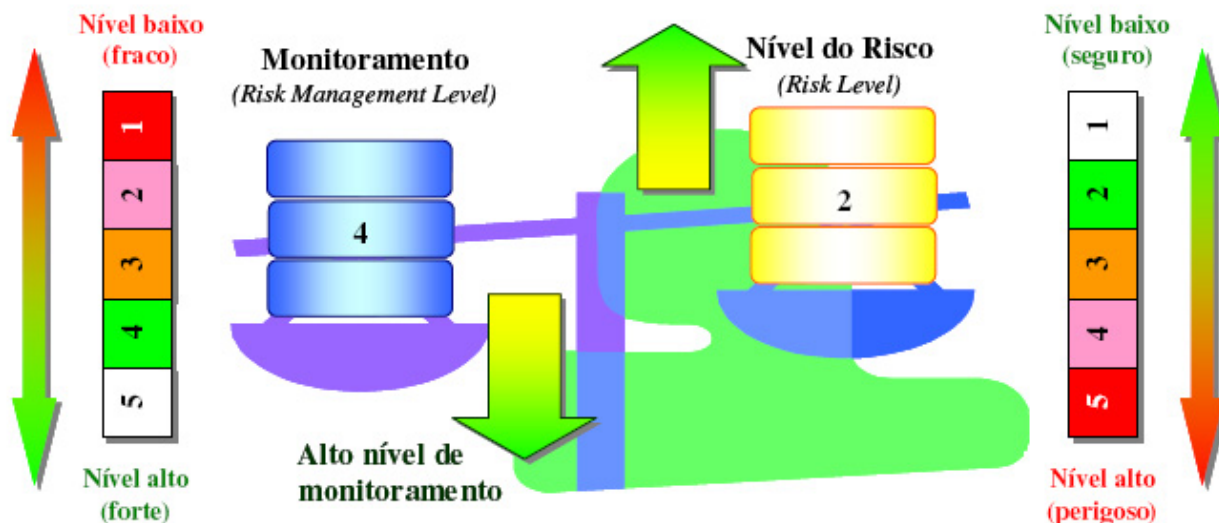
Segundo a norma, a PGR deve conter:

- a justificativa da organização para gerenciar riscos;
- as ligações entre os objetivos e políticas da organização com a política de gestão de riscos;
- as responsabilidades para gerenciar riscos;
- a forma com que são tratados conflitos de interesses;
- o comprometimento de tornar disponíveis os recursos necessários para auxiliar os responsáveis pelo gerenciamento dos riscos;
- a forma com que o desempenho da gestão de riscos será medido e reportado, e
- o comprometimento de analisar criticamente e melhorar periodicamente a política e a estrutura da gestão de riscos em resposta a um evento ou mudança nas circunstâncias.



Para a Brasiliano & Associados, o esqueleto básico de uma política de gestão de riscos, deve ser:

1. Objetivo
2. Definições
3. Descrição do Processo de Avaliação de Riscos
4. Avaliação do Nível de Riscos
5. Respostas aos Riscos
6. Priorização das ações
7. Monitoramento e Auditoria
8. Anexos – documentos e Modelos de Planilhas



Fonte: Brasiliano & Associados

## EXEMPLOS

Alguns exemplos de trechos da política de gestão de riscos de algumas corporações:

*“A Petrobras adota uma política de gestão de riscos restritiva quanto à utilização de instrumentos derivativos, limitando seu uso apenas a operações de proteção, sob rígido controle.”*

*“Na Novo Nordisk faremos a gestão do risco de forma a permitir o crescimento contínuo do nosso negócio e a proteger os nossos colaboradores, bens, lucros e reputação contra perdas materiais. Isto significa que iremos: Identificar e estabelecer os riscos materiais associados ao negócio; Monitorizar e atenuar os riscos, de forma a maximizar os benefícios de negócio; Utilizar uma gestão de risco comum, sistemática e integrada, enquanto é mantida uma flexibilidade de negócio.”*

*“A gestão dos riscos no Banco Intermedium é apoiada na ‘Política de Controles Internos e Gestão de Riscos’. Esta política contém as definições do Sistema de Controles Internos e Gestão de Risco, que consiste em um processo estruturado que abrange o Conselho de Administração, a Alta Administração, as Gerências e todos os Colaboradores da organização, com o objetivo de proporcionar uma razoável se-*

*gurança quanto à conclusão adequada e eficiente dos negócios para o alcance dos objetivos estabelecidos e a conformidade com as políticas, normas e regulamentações aplicáveis. Os papéis e responsabilidades de cada participante do Sistema de Controles Internos e Gestão de Riscos, e as definições de segregação de funções e conflito de interesses encontram-se descritos na política, sendo sua execução apoiada pela estrutura de Controles Internos e Gestão de Riscos.”*

## CONCLUSÃO

De forma geral, os riscos têm se diversificado e aumentado. Uma nova maneira de encarar essa realidade é aceitando-os como oportunidades, visando a criação de um sistema de gerenciamento fortalecido, assim como o crescimento e a prosperidade da corporação.

Ao mesmo tempo, as corporações devem cumprir suas responsabilidades com relação aos seus stakeholders com o objetivo de conquistar a confiança dos clientes com relação à(s) sua(s) marca(s).

Sem política de gestão de riscos, não há gestão de riscos.

**Mariana Fernandez**

Editora

sumário



# A Importância de Gerenciar Riscos de Compliance nas Corporações

Antonio Celso Ribeiro Brasileiro

## I. CONCEITO E ORIGEM

O termo *compliance* origina-se do verbo inglês *to comply*, que significa cumprir, executar, satisfazer, realizar algo imposto. *Compliance* é o ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da organização, buscando diminuir o risco atrelado à reputação e ao regulatório/legal.

Diante do contexto da dinamicidade do mundo globalizado e sua extrema velocidade e agilidade surgiu a necessidade de regulação e de padrões de transparência, tendo como consequência direta a criação de *Compliance – Conformidade*.

A área bancária brasileira hoje, é uma das instituições mais reguladas, tendo inclusive a partir de 1990, com a abertura comercial e o Brasil conquistando espaço no cenário mundial da alta competitividade, surgiu pressão para o alinhamento a padrões internacionais de transparência e de segurança adotados pelos órgãos reguladores.

Em 1997, o Comitê de Basiléia divulgou orientações aos bancos centrais para garantirem, na medida do possível, a rigidez dos sistemas financeiros, com responsabilidades e objetivos bem definidos. Os bancos brasileiros, nessa mesma época, enfrentavam o aumento da competitividade em busca de um percentual de representatividade no mercado. Enfrentavam também a falta de adequação de controles internos e não observância de princípios éticos, aumentando os riscos da atividade, o que, entre outros fatores, contribuiu para a quebra de alguns bancos.

Em 2001, com os atos terroristas nas Torres Gêmeas nos Estados Unidos e os escândalos financeiros mundiais, tais como Banco Barings, Enron, WorldCom, Parmalat, acentuaram a necessidade de regulação ainda mais efetiva e aplicável, a todos os países que procuram a mitigação de riscos.

Hoje, no Brasil, o compliance é estabelecido com o propósito de estar diretamente ligado às mudanças que visam alinhar processos e assegurar o cumprimento de normas e procedimentos por meio de um efetivo ambiente de controles, além de preservar a boa reputação da empresa perante o seu mercado.

## 2. RISCO DE COMPLIANCE

A expressão risco de compliance é definida 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.

Segundo Paul Argenti, Professor de Comunicação

Corporativa da Tuck School of Business – Estados Unidos, 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.

Essa avaliação fundamenta-se na identidade da empresa - incluindo informações sobre visão e estratégia, ações no decorrer do tempo, percepção por parte de pesquisadores e terceiros com credibilidade - e no desempenho, pela lucratividade e responsabilidade social.

O risco atrelado à reputação é, portanto, a perda potencial na reputação da empresa, podendo levar à publicidade negativa, perda de rendimentos, litígios caros, declínio na base de clientes e até falência.

A associação de bancos ABBI e a FEBRABAN estabelecem que compliance implica em:

- 1 – Leis: aderência e cumprimento;
- 2 – Princípios éticos e normas de conduta: existência e observância;
- 3 – Regulamentos e Normas: implementação, aderência e atualização;
- 4 – Procedimentos e controles internos: existência e observância;
- 5 – Sistema de Informação: implementação e funcionalidade;
- 6 – Planos de Contingência: implementação e efetividade por meio de testes periódicos;
- 7 – Segregação de funções: adequada implementação para evitar o conflito de interesses;
- 8 – Relatório do sistema de controles internos – gestão de compliance: avaliação dos riscos e dos controles internos – elaboração com base nas informações obtidas junto às diversas áreas



da instituição, visando apresentar a situação qualitativa do sistema de controles internos em atendimento à resolução número 2554, de 24/09/1998;

- 9 – Políticas internas: prevenção de problemas de não conformidade com leis e regulamentações.

As atividades acima descritas são bastante exaustivas e constituem importantes balizas na gestão de riscos de compliance.

Cabe ressaltar que uma ferramenta estratégica para a eficácia da gestão do risco de compliance é o seu monitoramento. O monitoramento propicia o acompanhamento do negócio e a identificação do risco regulatório a que esse está exposto. Propicia também identificar os controles de negócio que estão falhando e precisam de ações corretivas. O monitoramento de compliance deve ser devidamente documentado e reportado para a alta administração.

### 3. COMPLIANCE & ÉTICA

As estratégias mais eficientes para garantir o comprometimento são as que se baseiam em argumentos bem fundamentados. Segundo Janice Payan e McFarland Richard, autores de uma pesquisa nos Estados Unidos sobre fatores determinantes de influência na eficácia de estratégias e políticas, os argumentos influenciam muito mais do que simples recomendações. “Recomendação é, na essência, aconselhamento sem o suporte evidente” .

Os sistemas de compliance devem possuir dois componentes: poder e grau de comprometimento. Sendo poder conceituado como a habilidade de um ator induzir ou influenciar outro ator a seguir diretrizes ou normas que defende.

Compliance é uma questão de ética, devendo o programa de compliance auxiliar funcionários na resolução de situações não cobertas pela legislação. 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.

A ética deve fazer parte dos objetivos da empresa, presente nas decisões em diferentes níveis e incorporada à cultura da organização.

Programas relacionados a ética são justificados pela necessidade de conformidade com requisitos legais e de regulação. Além disso, agregam valor e benefícios à organização, pois aumentam a vantagem competitiva, reduzem riscos e constroem um relacionamento mais confiável com o mercado. Igualmente, auxiliam os funcionários em seus julgamentos e contribuem para a construção de relações de respeito e de confiança, o que torna melhor o ambiente social de trabalho da empresa,



influindo positivamente sobre a produtividade. Os programas devem conter os seguintes elementos:

- apresentar e discutir com os profissionais os aspectos éticos envolvidos nas práticas das empresas;
  - desenvolver código de ética da empresa;
  - capacitar os profissionais na abordagem de questões éticas;
  - criar canais de identificação de condutas não-éticas e formas adequadas de aconselhamento.
- DISQUE DENÚNCIA.

A existência de um código de ética bem estabelecido pode contribuir para que o compliance atinja seus objetivos. Portanto, há a necessidade dos programas de divulgação dos respectivos códigos de ética e seu monitoramento através dos canais de comunicação abertos para que quaisquer violações ao código possam ser reportadas.

#### 4. COMPLIANCE & AUDITORIA

O *The Institute of Internal Auditors – IIA* – Estados Unidos, conceitua auditoria interna como sendo uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações de uma organização; além disso, assiste à organização na consecução dos seus objetivos por meio de abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de risco, do controle e dos processos de governança.

A auditoria interna efetua verificação de forma aleatória e temporal por meio de amostragens para certificar-se do cumprimento das normas e processos instituídos pela alta administração. Já o compliance, executa tais atividades de verificações de forma rotineira e permanente,

monitorando-as para assegurar, de maneira corporativa, que os departamentos e unidades estejam respeitando as regras aplicáveis a cada negócio; ou seja, cumprindo as normas e processos internos para a prevenção e controle dos riscos envolvidos em cada atividade. Compliance é um braço dos órgãos reguladores junto à administração no que se refere à preservação da boa imagem e reputação e respeito às normas e controles, na busca da conformidade.

Compliance deve ser tão independente quanto a auditoria, reportando-se à alta administração para informá-la de eventos que representem riscos de compliance, ou seja, regulatório, e que possa afetar a reputação. Compliance engloba o acompanhamento dos pontos falhos identificados pela auditoria até que sejam regularizados, configurando intersecção das duas áreas. Apesar de ter funções semelhantes, o compliance faz parte da estrutura de controles, enquanto a auditoria avalia esta estrutura.

Auditar compliance significa compreensão da cultura de conformidade e seu grau de comprometimento dos profissionais.


#### 5. COMPLIANCE & GOVERNANÇA CORPORATIVA

O consultor de empresas João Bosco Lodi afirma que a era da governança corporativa começou em 1992, época em que foi derubado Robert Stempel, diretor presidente da GM e do conselho de administração. Sua queda provocou reações, tornando mais atuantes os conselhos de administração de outras grandes empresas.

Em 1991 foi lançado nos Estados Unidos o livro *Corporate Governance*, de Robert A. G. Monks, que via a governança corporativa como uma hélice dupla, que enxergava um relacionamento humano responsável e







construtivo das empresas com a sociedade e com o lucro. De acordo com Monks , as empresas que tivessem atitudes adequadas permaneceriam por muito tempo e se tornariam mais resistentes aos impactos das crises e recessões da economia.

Hoje, é impensável fazer governança corporativa sem o compliance. Compliance contribui para a governança corporativa à medida que fortalece os controles internos da empresa, mitiga os riscos atrelados à reputação e riscos de sanção regulatórias, disseminando elevados padrões éticos. Sem ética não há governança corporativa, uma vez que os padrões éticos e a indispensável interação das práticas de governança colaboram para que a corporação atinja seus objetivos e perenidade no mercado. Isso é sustentabilidade empresarial!!

## 6. CONCLUSÃO

A gestão de riscos corporativos possui em seu portfólio de atuação o risco de compliance, cabe agora aos gestores de riscos possuírem capacitação e tecnicidade.

A falta de capacitação de gerir riscos de compliance pode acarretar consequências

graves para as empresas. Numa 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 e o compliance é um deles.

O gestor de riscos deve ter em mente que, em geral, se administra as ameaças concretas em detrimento da reputação, o que não é gestão de riscos e sim de crises. Há a necessidade de focar na gestão proativa de riscos reputacionais, pois sem gestão desses riscos as empresas podem ter desde danos à reputação da empresa e marca até a cassação da licença de operação.

O principal desafio é, portanto, reconhecer o risco reputacional como uma categoria distinta de risco, por essa razão é que o Compliance está se tornando um fator de competitividade à medida que, cada vez mais, a busca pela transparência, ética e conformidade aumenta. Só assim será possível criar uma verdadeira vantagem competitiva, desenvolvendo um conhecimento detalhado da regulação do negócio.

**Antonio Celso Ribeiro Brasileiro**

Publisher da Revista Gestão de Risco

e Diretor da Brasileiro & Associados

[abrasiliano@brasiliano.com.br](mailto:abrasiliano@brasiliano.com.br)

sumário

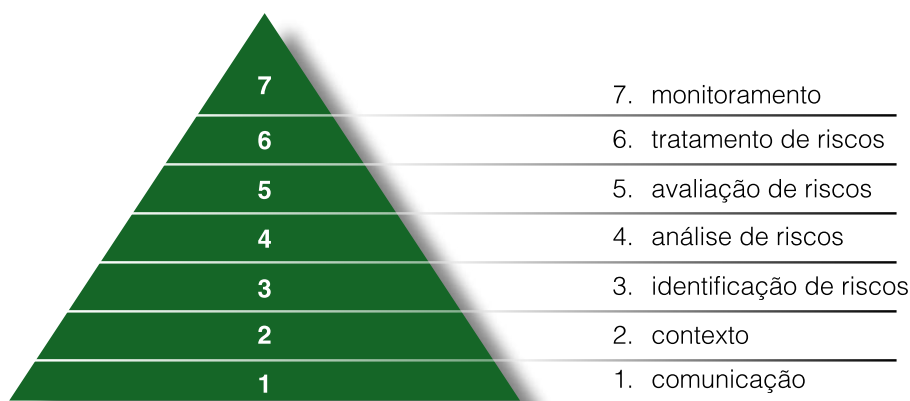


## Serviços de Consultoria **Plano de Gestão de Riscos Corporativos - PGRC**

### **Sua empresa conhece o TAMANHO de seus riscos??**

Um PGRC é um processo estruturado para que a empresa possa identificar eventos que expõem os objetivos da organização.

O processo de Gestão de Riscos, hoje é estruturado com base na futura ISO 31000.



**A Brasileiro pode ajudar você a elaborar seu plano de PGRC**  
**Consulte – nos!!!!**

informações | 11 5531-6171  
| [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)



# Destrinchando a PERÍCIA eletrônica – Parte 2

Mariana Fernandez



Qualquer pessoa pode tornar-se um perito eletrônico? Quais são as faculdades essenciais do profissional? Que formação o perito digital deve ter? Quais as diferenças da investigação tradicional para a investigação pericial? Tudo isso e muito mais você irá saber na continuação da entrevista especial sobre Perícia Eletrônica com o professor, perito e Presidente do Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática, Giuliano Giova.

Giova atuou como executivo e profissional de processamento de dados por 25 anos, tendo sido por mais de dez anos gerente de desenvolvimento de sistemas do Banco Itaú. Economista e especialista em informática, o perito é conselheiro do Conselho de Comércio Eletrônico da Federação de Comércio do Estado de São Paulo e membro dos comitês sobre telecomunicações, tecnologia da informação, e-bussines e direito da tecnologia, da Câmara Americana de Comércio. presidente da Conferência sobre Fraudes e Crimes Corporativos (Unicorp), presidente da Conferência sobre Riscos Legais em Empresas no Uso de E-mail e Internet (ADPO)

Como professor, é docente no curso de extensão universitária em Prova e Perícia Eletrônica da Brasiliano & Associados além de muitos outros.

A seguir, GG fala da perigosa via de mão-dupla dos softwares piratas, dos riscos dos sites pornográficos e da formação pericial em geral.

---

**O que fica mais difícil: evitar que aconteçam fraudes, impedir o ataque de hackers ou pessoas que roubam informações ou identificar os criminosos? Qual dessas três coisas é mais difícil para um perito?**

É importante estabelecer uma diferença entre o profissional de segurança da informação e o perito. O profissional de segurança da informação atua preventivamente, é ele que estabelece políticas de segurança na empresa e monitora essa segurança através de ferramentas, através de recursos de proteção e assim

por diante. No momento em que ocorre um incidente, uma invasão, uma sabotagem, um furto, esse profissional de segurança da informação investiga esse incidente mas quando se aproxima de uma posição jurídica em que haverá um processo jurídico ou uma denúncia policial, um inquérito policial, a rigor, é onde bastão é passado para o perito. Evidentemente, as coisas não são assim tão fáceis de serem separadas. A rigor, as duas coisas são muito próximas. Vou dar um exemplo: ainda hoje a maior origem dos problemas da Internet são os contos do vigário modernos, são as novas facetas do conto do vigário. Por exemplo, a pessoa que cai na tentação de instalar um Windows pirata no computador porque alguém disse pra ela que é mais barato. O que ocorre é que o Windows pirata obviamente é muito vulnerável, terrivelmente vulnerável a qualquer ataque. Porque o Windows, quando é fabricado, ele sai de fábrica com um monte de defeitos, porque ele é muito grande, muito complexo. Só que a Microsoft corrige em tempo real esses defeitos na nossa máquina e fica monitorando e corrigindo. Só que se software é pirata ele não vai corrigir obviamente. Então o que acontece, a pessoa se acha esperta no momento em que ela diz “coloquei um software sem gastar nada” mas evidentemente ela vai ser pega, ou porque alguém furta a senha dela ou porque alguém invade o computador dela e rouba um segredo. E aí nós sabemos a longa lista dos golpes do vigário: um e-mail “dizendo eu te amo”, “você ganhou um prêmio” e assim por diante. E, finalmente o site pornográfico: santo Deus, ninguém mantém na internet gastando dinheiro do seu bolso site pornográfico só para os outros terem prazer, obviamente esse sites pornográficos têm dispositivos, artefatos maliciosos para contaminar o computador de quem os visita. Então em essência é isso: a gente tem essa dualidade das pessoas que na internet se acham espertas entre aspas, acham que vão conseguir vantagens, só que nessa de conseguir vantagens elas viram vitimas.

---

### **Qual é a vantagem de se contratar um perito eletrônico no lugar de um detetive particular quando se vai rastrear crimes e buscar pessoas desaparecidas?**

Eu acho que as duas coisas se complementam Mariana. Eu acho que são faces distintas... porque se uma pessoa desapareceu ou não apareceu pode ser de diversas maneiras: ou porque se perdeu o contato a muitos anos atrás ou principalmente porque foi sequestrada qualquer coisa assim. O detetive tradicional, o detetive do mundo real é sempre alguém extremamente importante, desde de que, evidentemente, seja ético e competente. Porque ele tem competência para entrevistar pessoas, tem competência para seguir rastros e assim por diante, que muitas vezes demandam uma atuação presencial. Esse mesmo detetive, hoje em dia, também utiliza a internet, usa Google, utiliza serviços diversos, catálogos telefônicos, serviço 102 e assim por diante. Então não é que o detetive tradicional não use meios eletrônicos, mas é completamente diferente do perito. O perito vê esse mundo digital com outros olhos. Por exemplo, se é necessário examinar o disco rígido da pessoa desaparecida em busca de evidências e contatos que essa pessoa teve no MSN, Skype, que possam levar à sua localização, então entra aí o perito eletrônico. Em outras situações, no momento em que ele precisa vasculhar a internet com tecnologias mais sofisticadas, por exemplo, procurando uma imagem específica dessa pessoa para ver se a foto dela está em algum lugar, não é o detetive que vai conseguir fazer isso. Sempre que se envolve uma tecnologia mais profunda é papel do perito eletrônico estar atuando nessa parte. Acho que as duas coisas se complementam...

---

### **São funções um pouco diferentes...**

Exatamente. São complementares.

---

### **O senhor trabalhou no banco Itaú na área de desenvolvimento de sistemas por mais de 10 anos...**

Na verdade por quase 30 anos...

---

## **E isso auxiliou, influenciou de que maneira senhor para que se tornasse um perito eletrônico?**

Foi de uma importância fundamental porque o perito eletrônico tem que usar uma mentalidade científica. Isso é extremamente importante. Por isso nós temos visto esses filmes na TV canais única e exclusivamente ou quase que exclusivamente de filmes sobre perícia: na área médica, na área criminal. Então a gente percebe que o perito, hoje em dia, tem que ser um cientista, e não precisa ir muito longe é só ver os números que eu te dei... processam-se dois milhões de instruções por segundo e guarda-se cento e sessenta bilhões de dados... é coisa pra cientista. Por isso esses peritos têm que ter uma mente preparada para esse tipo de coisa e ao trabalhar numa grande empresa de nível sofisticado de tecnologia, prepara-se esse jovem, prepara-se a mente dessa pessoa para esses desafios. Nós temos participado em casos muito importantes, auxiliando as autoridades na busca de criminosos, na busca de pessoas que cometeram atos ilícitos ou ações indevidas em ambientes super sofisticados e se a gente não tem essa separação não conseguimos... então essa formação da grande empresa, da empresa que adota padrões sofisticados de trabalho é fundamental para o perito.

---

## **As pessoas que já estão trabalhando na área eletrônica e querem partir para essa área mais científica da perícia como analistas de sistemas, cientistas da computação, o que eles devem fazer ou que formação ele devem buscar ter para ir para área da perícia?**

Hoje existem muitos cursos de pós-graduação nessa área. Começando pela própria Universidade de São Paulo que tem mestrado em Engenharia Legal. As diversas universidades... Mackenzie, Impacta, todas essas têm cursos de extensão, cursos de pós-graduação na área de tecnologia, área de perícia. Então isso é uma coisa fundamental. Outra coisa que é muito importante, são as certificações que são próprias da área de segurança da informação. Nós vimos que há uma diferença na área de segurança da informação e perícia, é uma questão de fazer esse trabalho. Mas os conhecimentos são muito próximos. Hoje, muitas empresas, muitos fabricantes de softwares, muitas empresas de treinamento, elas certificam os profissionais quanto à sua competência, isso é muito bom para o perito também. É importante ele estar disponível aí na internet. Qualquer pesquisa mostra dezenas ou centenas de cursos disponíveis nessa área. Finalmente, eu acho extremamente importante que a pessoa tenha interesse nisso, participe de fóruns... tem fóruns na internet abertos, gratuitos onde basta a pessoa se inscrever. São sobre perícia forense, perícia computacional. Então ela tem que viver isso, ela tem que se inscrever nisso e participar dos debates. Isso é muito esclarecedor quanto à evolução da carreira e para que a pessoa saiba se realmente ela tem interesse nisso.

---

## **Com relação ao curso que o senhor é também professor de própria perícia eletrônica da Brasileiro, qual é a disciplina lecionada pelo senhor e qual profissional pode estar participando do curso?**

Primeiro grupo são os profissionais que querem atuar com perícia. Esses, com certeza, devem participar do curso. O segundo grupo são todos aqueles profissionais ou atuam na segurança da empresa ou na gestão da empresa. Por que isso? Porque, antigamente, era comum, que quando acontecia algum incidente dentro da empresa, a empresa escondia, porque ela achava que a divulgação de algum problema na empresa podia denegrir a imagem da empresa. Só que isso se mostrou ser um poço sem fundo, porque algum funcionário aprontou alguma coisa e a empresa não tomou nenhuma atitude mais firme os outros

que estão sabendo disso, que estão presenciando isso, são os candidatos a reiterar, a refazer esses comportamentos indevidos. Então, hoje em dia, mudou radicalmente. A primeira era em bancos, que, tradicionalmente, ocultavam qualquer problema. Hoje sempre se toma uma atitude mais firme. Então é extremamente importante que estes gestores, estes profissionais que gerem pessoas e o pessoal de segurança da informação saibam o que se faz em termos de perícia. Temos visto aí coisas que são extremamente importantes a serem transmitidas para esse pessoal. Vou dar um exemplo muito claro que durante as minhas aulas as empresas ficam espantadas. São coisas muito simples. Então imagine o seguinte: toda empresa tem pelo menos um ou dois computadores dedicados a fazer transações bancárias, tem o computador da área financeira onde se faz, por exemplo, contas a pagar. E, existe uma providência extremamente simples, extremamente banal, de segurança para esses computadores que é o seguinte: nunca envie ou receba e-mail por esses computadores. Hoje o custo de um computador é tão baixo que você pode dedicar um computador única e exclusivamente para acessar bancos. É uma providência extremamente simples que aumenta muito a segurança das empresas. Você evita um ataque hacker que vai resolver a conta da empresa, mas ninguém percebe isso. Então, quando os profissionais de segurança de informação, o pessoal de segurança patrimonial, os gestores, os gerentes, diretores de empresas participam desses cursos da Brasiliano, com certeza saem enriquecidos, aumentando e muito a segurança da empresa.

---

### **Qual a disciplina lecionada pelo senhor no curso?**

Perícia eletrônica. Varia um pouco o nome em função da extensão do curso mas a essência é prova e perícia eletrônica.

---

### **Sobre o instituto, como os peritos podem fazer parte do instituto? Existe essa possibilidade ou já é um conjunto de peritos fechado ?**

Nós temos dois grupos. O primeiro é de funcionários que são já peritos associados e que atuam permanentemente junto ao instituto. O segundo grupo é de peritos colaboradores, ou seja, de peritos que colaboram para eventos específicos. Por exemplo, uma perícia específica que eles querem ou que o perito quer fazer junto com a gente ou precisa usar nosso laboratório ou queira trocar experiências tirar dúvidas... aí sim essa seção de colaboração. Prevejo ampliar esse procedimento para promover a proximidade de peritos de qualquer parte do país participando do instituto... mas isso ainda está em gestação, ainda vai demorar mais um ano.

---

### **Sobre a qualificação dos peritos eletrônicos, como existem dois tipos que o senhor me explicou, os peritos com formação na academia de polícia e os peritos judiciais, esses últimos são, hoje, satisfatoriamente qualificados ou senhor acha que eles poderiam ser melhores?**

A formação de quase todos os peritos é insuficiente e precisa urgentemente ser melhorada. Vamos pensar um pouquinho no que é o Brasil. Isso é uma coisa muito séria... pensa comigo: nós temos hoje, aproximadamente acho eu, doze mil peritos no Brasil e uma boa parte desses peritos pertence a nove mil varas, tribunais que existem no Brasil. Então se você pensar em cada comarca dos estados do Brasil você vai ter ali um, dois, três, quatro peritos. Ocorre que esse pessoal não tem recursos, não tem acesso a quase nada mais. Em contrapartida, no interior, você vê computadores realmente sofisticados pois qualquer fazendeiro tem seu Mac, PC ou notebook e assim por diante. O que acontece? Houve um distanciamento

muito forte entre a preparação desses peritos há quatro, cinco anos atrás e a realidade dos equipamentos a serem apreciados hoje em dia nesse mundo de fora. Então isso leva a uma situação muito grave que é falta de fundamentação no laudo pericial. Por que? Porque o perito recebe a missão do juiz, examina o computador, não sabe bem o que ele viu e chega muitas vezes a uma conclusão que não é fundamentada. O que acontece? A definição do laudo pericial seja do Aurélio ou do CREA, todos os diversos conceitos batem no mesmo ponto, que o laudo pericial tem que ser fundamentado, ou seja, ele tem que dizer porque chegou àquela conclusão. “A Mariana enviou ou não enviou e-mail?” Não basta dizer se enviou ou não enviou, tem que demonstrar porque. Por quê o perito chegou a essa conclusão. E é aí que está o perigo. A partir do momento em que o perito não é adequadamente preparado, é um chute, é como “jogar moedinha pra cima”. Essa grande dimensão territorial, essa grande quantidade de peritos no espaço do Brasil inteiro de um lado, por outro lado essa rápida evolução da tecnologia da informação, da telecomunicação, cria um distanciamento muito grande, então faz com que realmente os peritos não estejam preparados para isso. Esse é um dos pontos pelos quais o Brasileiro está sendo pioneiro no lançamento do curso à distância, curso online que virá realmente de encontro a formação desses milhares de peritos do Brasil inteiro, tanto os candidatos a perito quanto os que já são.

---

**Quais são as faculdades, alguma característica da personalidade de uma pessoa para se tornar um(a) perito(a) ou o que ela deve agregar ao que ela já é para que ela seja um bom perito ou boa perita?**

A atividade do perito é regulada tanto pelos códigos de processo penal e código de processo civil como pelos provimentos, os mandamentos dos conselhos superiores dos tribunais. Todos eles em comum dizem a mesma coisa: o perito não pode ter sido condenado, não pode ter dívidas, tem que ter um caráter... ser uma pessoa absolutamente confiável, ser uma pessoa íntegra, eficiente... no fundo ele está representando o juiz...

---

**São praticamente os mesmo atributos...**

Isso exatamente! Muito bem posto! Ele tem que ter essas características de isenção. Ele tem que se declarar impedido, caso ele veja algum conflito de interesses. Exemplos: se eu trabalhei na Coca-Cola eu não posso ser perito de uma ação contra ou a favor da Coca-Cola. Se eu devo dinheiro à Coca-Cola eu não posso atuar no caso dela. Então todas aquelas condições de suspensão e de impedimento do juiz se aplicam também ao perito. Essas características pessoais do perito são fundamentais porque ele não só tem que ser de confiança do juiz como ao fato. Afinal, se duas empresas, duas pessoas, estão recorrendo ao judiciário em função de algum litígio e esse litígio vai ser resolvido pelo perito, ele tem que ter compostura, tem que ter conhecimento, tem que se impor à essas partes, no bom sentido, fazendo com que elas confiem nele, na sua avaliação e na sua decisão. Então essa característica pessoal é fundamental pois se uma pessoa não é tão íntegra, ela não pode ser perito.

---

**Com relação às habilidades das pessoas, além de entender bastante a área tecnológica e ter experiência prática nisso que outras habilidades deve ter, que tipo de conhecimento deve ter pra auxiliar na profissão?**

Além de dever ter noções de direito, o perito tem que enxergar dois grandes sistemas. Tem que enxergar e compatibilizar de um lado o chamado sistema tecnológico. O que é o sistema tecnológico? Imagine um

perito examinando um produto bancário. Primeiramente tem que se entender que esse produto bancário nasce lá no Banco Central, na norma do Banco Central, aí vai descendo... esse produto bancário numa certa altura vira tela dos computadores e arquivo dos computadores, vira programas, transações que o usuário faz, termina lá no caixa eletrônico, termina numa memória de computador. Mas tudo isso deve ser enxergado pelo perito de uma forma ampla. E do outro lado ele tem que enxergar o sistema jurídico, porque tudo que se refere à tecnologia, muito provavelmente, está envolvido com direito internacional, gente lá de fora, componentes estrangeiros. Aí chega nas condições típicas da Justiça no Brasil e vai descendo pelo sistema de normas da Justiça até o momento em que se aplique especificamente no que está sendo periciado. Essa junção desses dois mundos é a grande habilidade que o perito tem que ter. Ele tem que enxergar esses dois mundos, avaliar os acontecimentos entorno disso e ser líder dessas partes, dos assistentes técnicos, das duas partes, de maneira a fazer com que se tenha um trabalho produtivo. Porque imagine se eles começarem a brigar: “eu tenho razão!”, “não, eu é que tenho razão!”. O perito tem que ter habilidade interpessoal para poder coordenar esse trabalho e fazer com que se chegue a atividades produtivas e a um resultado palpável para o juiz.

---

**Com relação a hackers, softwares ou vírus que se instalam nos computadores e leem as informações e também em relação às novas tecnologias: como é que os peritos devem se atualizar para conseguir acompanhar tanto a tecnologia quanto a tecnologia que é utilizada contra os usuários?**

Aí você toca num ponto grave. É a famosa briga do entre os chamados hacker e cracker. As pessoas, em geral, ela dividem o cracker do hacker, separam os conceitos. O hacker seria o jovem que estuda, o autodidata que conhece os termos operacionais, conhece a rede de computadores e assim por diante “para o bem”. E o cracker seria aquele que faz o mal. Eu não compartilho disso, eu me comporto. Acho que o que acontece na prática é que o hacker é o cracker trainee porque ele acaba mais cedo ou mais tarde tentando invadir os computadores alheios, tentando invadir as redes alheias. Eu, realmente, não compactuo dessa visão do hacker. Eu acho que o lugar do jovem é na universidade. Quem gosta de tecnologia tem que fazer curso de graduação, tem que fazer pós-graduação e os experimentos não podem ser feitos no escurinho do seu quarto. Essa estória de estar no escurinho do quarto estudando tecnologia da informação é, provavelmente, invadindo a rede da operadora de telecomunicações ou o computador do vizinho. Isso não funciona, isso não pode ser assim. Isso é a escola do rapaz que vai ser aliciado pela quadrilha organizada. A quadrilha organizada, hoje em dia, descobriu que é muito melhor aliciar um jovem e ele fazer um furto do que sair de metralhadora em punho assaltando agência bancária, é mais arriscado fazer isso. Aquele jovem que se acha o hacker, ele é o próximo a ser aliciado por essas quadrilhas. Por isso os pais têm que acabar com essa estória. Lugar de jovem que gosta de computador, de tecnologia é na universidade, ou numa grande empresa aprendendo.

---

**Existe demanda suficiente de trabalho para os peritos não apenas na área judicial mas às vezes sendo contratados por empresas para descobrir alguma fraude? Existe essa demanda ou a área acadêmica é melhor opção para um perito?**

É as duas coisas são verdadeiras. Tanto se tem a demanda da investigação particular, porque, normalmente, a investigação particular acaba virando judicial lá na frente. Na medida em que se encontra a fraude, em que se encontra o ato devido, ele acaba indo para o departamento jurídico, daí acaba virando uma ação efetivamente judicial. Assim como nas próprias universidades, a pesquisas nessas áreas são extremamente



importantes. A gente percebe, hoje, que o computador está embutido em todos os dispositivos. O tal do desktop é fim de carreira, ninguém mais quer o desktop. O computador, hoje, está escondido no celular, está escondido na geladeira, ele está escondido no automóvel, no semáforo, no acesso controlável, ou seja, toda nossa sociedade, hoje em dia, funciona com base no computador e é exatamente aí que se tem a necessidade de segurança, a necessidade de se verificar o sistema para que ele seja confiável nos termos requisitos e que ele seja seguro.

---

### **O volume de trabalho é maior na área judicial, nas corporações ou particulares para pessoas físicas?**

É, o particular está tendo uma demanda muito forte. Por exemplo, as pessoas hoje se esquecem que os celulares deles são um computador. Em muitos casos, por exemplo, o namorado filma o corpo da namoradinha etc e tal e aquilo fica gravado na memória do celular, só que um belo dia ele esquece disso e entrega o celular para o dono da assistência técnica, daí é um passo para que alguém encontre esses filmes íntimos e jogue isso na internet. Temos visto aí grandes desgraças rolando cada dia mais. Além da tal webcam. É normal, hoje em dia, que a garotada faça coisas via webcam esquecendo-se que do outro lado podem estar sendo gravados. Então essa questão da privacidade pessoal, filmadoras em tudo, em banheiro de escola e assim vai, está pegando fogo! A violação dessa privacidade é o crime e as consequências são extremamente sérias, mas parece que as pessoas não se apercebem disso. Outra área muito forte é a da difamação. As pessoas acham muito fácil fazer um e-mail criticando um colega, um amigo, uma empresa e aquilo vai embora um passa para o outro e isso se propaga só que tudo isso é rastreado, é investigado e aí as pessoas são processadas. Na maioria das vezes elas não tinham noção do tamanho da encrenca em que elas se meteram ao fazer isso. Então essa área está pegando fogo. Tem o lado das empresas: houve uma queima muito grande no comprometimento entre funcionário e empresa. Antigamente o funcionário podia ficar 20 anos, 30 anos numa empresa e tinha um acordo tácito: a empresa protegeria o funcionário e este vestiria a camisa da empresa. É comum que o funcionário desenvolva uma carteira de clientes que, ao sair da empresa, ele ache que tem o direito de levar junto, o que não é verdade já que esta foi desenvolvida para a empresa... e por aí vai. O leque, hoje em dia, é infinito de problemas que são associados aos computadores e aos telefones celulares.

---

### **O caso da Catho em que o senhor participou e que resultou de um relatório de cinco mil páginas. Num caso como esse, qual é a melhor habilidade de um perito para desempenhar com responsabilidade sua função?**

Eu não posso falar especificamente do caso da Catho porque ele ainda está em julgamento. Mas em casos como esse, é extremamente importante a competência técnica, porque há tanto as organizações quanto as pessoas físicas, hoje, dispõem de tecnologia muito sofisticada para o bem e para o mal. Então, a investigação, o rastreamento e a produção de provas nesses ambientes requerem que o perito seja muito habilidoso e que atue de forma muito próxima ao juiz acima de tudo. O perito tem que ser os olhos e os braços do juiz. Então é extremamente importante que o perito siga estritamente o que o poder judiciário lhe determina.

---

### **Com relação à ameaças, os peritos também sofrem ameaças como alguns advogados na área criminal sofrem?**

Olha, comigo nunca ocorreu porque nossa visão é técnica, é uma coisa muito assim “é branco ou é preto?”, “tá ligado ou tá desligado?”, “é um bit ou é um bite?”. Percebe? Imagine você um médico ou um biólogo

que está analisando um DNA para determinar a paternidade ou a falta dela ser ameaçado. Não tem muito sentido. Entende? Até porque o que perito acha, ainda estará sujeito ao contraditório das partes, pois cada parte ainda vai ter o direito de se manifestar e criticar isso, e, evidentemente está sujeito ao julgamento do juiz. O juiz não é obrigado de forma alguma a decidir conforme o laudo pericial. O laudo pericial pode achar uma coisa e o juiz pode achar outra. Então, particularmente, até hoje, nada ocorreu.

---

### **E como que os peritos conseguem ser reconhecidos na profissão? Reconhecidos a ponto de serem escolhidos e contratados pela competência deles?**

Eu acho que é boca à boca. Boca à boca especialmente entre os colegas. Afinal, a perícia é um grande debate técnico. E pelos próprios juízes. Eu acho que é uma questão de uma soma de trabalhos bem feitos como da mesma forma trabalhos mal feitos denigrem rapidamente o perfil do perito. Então se se somar trabalhos bem feitos, se consegue o conhecimento do meio.

---

### **Agora eu preciso perguntar uma pergunta meio óbvia, que é se o senhor se sente realizado na sua profissão?**

Completamente! É algo desafiador. Esse talvez seja um ponto importante na sua entrevista... imagine você que um profissional seja um programador de uma determinada linguagem de empresa. A possibilidade é muito forte de que esse profissional fique seis meses ou um ano, cinco anos, dez anos fazendo a mesma coisa: programando naquela linguagem. Na perícia não. A cada dia um novo desafio absolutamente novo, um novo caso, novo ambiente, com novas dublagens, com novas ferramentas. A perícia é realmente, adrenalina pura!

---

### **E que conselhos o senhor daria para os novos ou ingressantes na perícia, principalmente na perícia eletrônica, ou para quem almeja ser um perito?**

Tenho certeza que eles só terão sucesso se forem muito dedicados ao estudo. É obrigatório fazer cursos, é obrigatório participar dos eventos, é obrigatório ler muito, pesquisar muito. Não é possível atuar nessa atividade estando isolado do mundo. Tem que evoluir, tem que se aperfeiçoar o tempo todo.

**Mariana Fernandez**

Editora

sumário

# ACONTECE

na *Brasiliano*

Mariana Fernandez

## BRASILIANO NO SUL



### PALESTRA SOBRE GRC NA TERRA DOS FARRAPOS

No último dia 15 de setembro, a *Brasiliano & Associados* realizou uma palestra esclarecedora sobre a ISO 31000 na capital Porto Alegre.



A palestra de tema *Gestão de Riscos Corporativos - Desafio com a Nova ISO 31000*, foi ministrada pelo especialista em GRC, Antonio Celso Ribeiro *Brasiliano* e foi muito proveitosa para os 122 participantes, colaboradores de empresas como AMBEV, Banco do Brasil, Banco do Estado do Rio Grande do Sul; Barra Shopping Sul, Correios, Gerdau, Itaú-Unibanco, Lojas Renner, Schincariol, Secretaria da Segurança Pública RS, Souza Cruz e Vivo.



Ocorrida no auditório do Complexo Operacional dos Correios, o evento desenvolveu temas como: contexto em que a ISO 31000 foi elaborada, consenso entre países, framework da norma, metodologias e ferramentas de GR.



A *Brasiliano & Associados* agradece a presença marcante dos participantes gaúchos no evento.

## EVENTOS EM CURITIBA

Em Curitiba a Brasileiro & Associados esteve presente nos dias 7, 8 e 9 de outubro, ministrando o Curso de Extensão em Investigações e Fraudes Empresariais para 23 alunos de empresas como HSBC, COPEL, Casas Bahia, Philip Morris, Sadia, Banco do Brasil, Wal Mart e Souza Cruz.



No Hotel Deville Curitiba, foram lecionados temas como Taxionomia das Fraudes Empresariais, Investigação Empresarial, Técnicas de Investigação Empresarial, Ética e Noções de Direito e Técnicas de Elaboração de Relatório.



Segundo o Prof. Antonio Brasileiro, as 24 horas/aula foram de um aproveitamento acima das expectativas.

No dia 8 de outubro, após o curso, o professor palestrou sobre riscos operacionais, na palestra intitulada Entendendo Riscos Operacionais. Com 93 inscritos e duas horas de duração, o evento foi debatido e aplaudido pelos presentes.



## BRASILIANO NO SUDESTE

### CURSO DE INVESTIGAÇÃO E FRAUDES EM TERRAS FLUMINENSES



Conforme observado pelo Prof. Antonio Brasileiro, houve um crescimento de interesse pela Fraude pelos profissionais da área de Gestão de Riscos.

E, conforme aconteceu em Curitiba, no Rio de Janeiro o Curso de Extensão em Investigações e Fraudes Empresarias foi um sucesso.



Nos dias 13, 14 e 15 de outubro, no Hotel Mercure Botafogo, 28 alunos de empresas como UFRRJ, UFPE, Sulamerica, Petrobras, Eletrobrás, CSN, Graber e Tv Globo, tornaram possível a proparagação do conhecimento da B&A na área de Fraudes para os profissionais fluminenses.



# BRASIL E ANGOLA,

AGORA JUNTOS NA GESTÃO INTEGRADA DE RISCO



Em 2008, a **Brasiliano & Associados**, através de um contrato de transferência de know-how da sua metodologia, processos e experiência abriu a **Brasiliano & Associados Angola**. A **Brasiliano & Associados Angola** é uma empresa 100% angolana, trabalhando com os mesmos padrões, moldes e processos da sua co-irmã brasileira. O objetivo é formar e qualificar consultores técnicos angolanos para estarem elaborando soluções na **Gestão de Riscos Corporativos**.

**COMPARTILHE DESTE DESAFIO!!!!**




**Sede Angola:** | Rua Comandante Kwenha, 2º edifício, 2º andar Cnj 21. Município das Kinachiche - Luanda - Angola

| Telefone Fixo: 244 222 008835 | Telemóvel: 244 914 656226 / 224 914 653224 / 244 929 529908 / 224 928 227713 / 224 923 609049

| e-mail: [riboldi@brasiliano.com.br](mailto:riboldi@brasiliano.com.br) / [mauro.ao@brasiliano.com.br](mailto:mauro.ao@brasiliano.com.br) / [dviana@brasiliano.com.br](mailto:dviana@brasiliano.com.br) / [abrasiliano@brasiliano.com.br](mailto:abrasiliano@brasiliano.com.br)

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



# FATO, métricas não quantificam o risco da informação

*Andre Pitkowski*

A vertical de mercado que põe mais pressão em seus profissionais de segurança é a do setor financeiro. A exigência dos executivos de negócio é para se quantificar os riscos da informação e o grau de exposição a que a informação está submetida.

Por quê? Nenhuma outra vertical de mercado sabe mais sobre riscos do que a vertical de serviços financeiros, e vocês, profissionais de segurança da informação, são permanentemente pressionados a trabalhar com mais rigor no âmbito da segurança da informação. No entanto, até o momento, as tentativas de atender esse nível de exigência tem sido, na melhor das hipóteses, (desculpem-me) medíocres.

Muitos dos modelos utilizados para se quantificar o risco da informação estão baseados em estimativas de modelos de estimativas (não está repetido, é isso mesmo!). A precisão é sempre mais um desafio que uma meta, e existe uma corrente de profissionais (colegas nossos) que acreditam que o verdadeiro risco de negócio não pode ser quantificado porque o que realmente está prejudicando o negócio é classificado como desconhecido pelos, especialistas no assunto

(ou então teríamos pelo menos uma resposta para cada um destes riscos).

É claro que se você estiver trabalhando no mercado financeiro, deve estar me considerando um cético, mas o fato é que no fundo você não está convencido de que realmente pode quantificar o risco da informação, mas também ainda precisa ser convencido de que não pode.

Acompanhe-me no raciocínio: Por que as grandes inteligências do mercado, com seus complexos modelos de risco, não conseguiram prever o estouro da bolha da internet? E o que dizer do desenrolar da festa de crédito fácil no fim de 2008? Se por um lado, o negativismo (ou pessimismo, como queiram) é ruim para o negócio, até aqueles especialistas respaldados por suas métricas foram pegos de surpresa (foram mesmo?), porque prever algo bom é que nem falar sobre a beleza de uma mulher atraente, ou seja, previsão sem embasamento é um exercício fútil e inútil.

Eu li “*O Cisne Negro*”, publicado em 2007 pelo ensaísta e pesquisador libanês radicado nos Estados Unidos, Nassim Taleb. Ele possui esse título porque, até o ano de 1697, os cientistas acreditavam que existiam apenas cisnes brancos, mas neste ano que descobriram um cisne negro na Austrália.

Nassim define no livro que o cisne negro é um acontecimento improvável e que depois do ocorrido, as pessoas procuram fazer com que ele pareça mais previsível do que ele realmente foi. No livro Nassim

escreve que é impossível tentar antecipar e prever o futuro, já que aquilo que conhecemos é muito menor em relação ao que não conhecemos. Ele também explica como uma pessoa deve lidar com eventos inesperados em um mundo imprevisível e que elas tenham a consciência e aceitem que esses eventos acontecerão numa hora ou noutra.

Nassim também usa alguns exemplos históricos para ilustrar os cisnes negros, como o atentado de 11 de setembro ao World Trade Center. Esse tipo de acontecimento possui três características principais: é imprevisível, causa um impacto enorme e depois de ter ocorrido surgem frequentemente diversas explicações que tentam afirmá-lo como menos aleatório e mais previsível do que na realidade é. Segundo Nassim, não temos consciência prévia desses fenômenos, dado que os seres humanos estão programados para aprender coisas específicas e não pensar em generalidades. Assim, não conseguimos avaliar claramente as oportunidades, nem somos suficientemente abertos para fazermos fé naqueles que conseguem imaginar o impossível.

Fechando esse parêntese, muito do que se discute, como a natureza da incerteza, tem a ver com o que estamos discutindo sobre métricas de segurança. Na ausência de um modelo preditivo verdadeiramente relevante, os especialistas passam muito tempo criando indicadores para todo tipo de riscos. A boa notícia é que existem muitos indicadores de riscos para contar, mas isso não significa que devemos contar todos eles.

Gente, eu não estou acusando as sofisticadas abordagens de modelagem de risco nem indo contra outras abordagens quantitativas como a FAIR (*FACTOR ANALYSIS OF INFORMATION RISK*). Para empresas conscientes de que suas informações são importantes e necessitam ser protegidas,







modelos como esse podem ser úteis. Eu estudei FAIR e conheço o mercado para pensar que menos de 5% das instituições financeiras se enquadraram nessa categoria. Desculpe-me se a pedra quebrou sua vidraça, mas antes de implementar sofisticados modelos de gestão de riscos, um pouco de bloqueio e combate faz bem e mostra serviço mais rápido.

Eu considero o uso de métricas em três categorias:

### **1. Relevância para o Negócio**

Estes riscos são mais qualitativos do que realmente quantitativos, mas podem ajudar os executivos a entenderem como e onde você está investindo seu tempo. A idéia aqui é fazer uso destas métricas para ganhar credibilidade e mostrar que você está no controle do programa de segurança. Aqui não se busca a excelência em registros operacionais; faremos isso mais abaixo.

Seu conjunto de métricas deve incluir o tempo de inatividade devido a problemas de segurança, número de dispositivos reinicializados após a ocorrência de um incidente, percentagem de código de programação que teve de ser revisado, etc. Lembre-se de que os executivos não querem saber dos detalhes mórbidos do incidente, a menos que explicitamente queiram. Geralmente, o que eles querem mesmo, é que você das uma pincelada do que você fez nas áreas atingidas pelo evento.

### **2. Resposta a incidentes**

É aqui que a cobra torce o rabo porque, como você, profissional de segurança responde a um incidente, tem tudo a ver com a manutenção do seu emprego amanhã.

Todos nós sabemos que incidentes acontecem, mas seu trabalho é conter os danos e reduzir a sobrecarga de responsabilidade que vai recair sobre a empresa. Claro que podemos fazer alguma coisa para prevenir que algo aconteça, mas quando acontecer você precisa saber o que fazer quando o número do indicador aparecer na mesa do executivo de negócio, e o que conta agora é o valor que vai ser atribuído a esse número, mais do que sua capacidade de resposta e do fato de que você deu o melhor de si para mitigar aquela situação.

As métricas aqui incluem o tempo médio para resolver um incidente, custo médio de um incidente, etc. Sob o ponto de vista de tendências, sua vontade é poder apresentar curvas decrescentes de tempo médio de resposta e custo médio de um incidente na medida em que você ganha experiência no assunto. Claro, você deseja também que o número absoluto de incidentes decaia, mas, sejamos realistas... esquece, nunca vi isso acontecer!

### **3. Métricas Operacionais**

Em última análise, grande parte do tempo de um profissional de segurança é dedicado a realizar as coisas que se ele sabe que funcionam. Por exemplo, instalando configurações de segurança em estações e servidores, instalando patches e hotfix (e isto toma muito tempo), monitorando redes e sistemas, etc. Reiterando o que eu escrevi acima, essas métricas são operacionais em sua natureza e prestam-se a fornecer indicadores cuja tendência deve ser melhorar ao longo do tempo.

Entenda que esse conjunto de métricas é para você, não para eles, os executivos. Sua gestão de negócio não se importa se você levou dois ou três dias para solucionar um problema com os servidores, contanto que

nenhuma informação tenha sido exposta ou perdida. Essas métricas são úteis sim, mas para melhorar o seu desempenho e sua eficiência. Já que temos que fazer essas coisas, pelo menos vamos fazer bem feito.

Me diga, como você “vende” esses tipos de métricas para os executivos de negócio? Será que eles estão interessados em ver seus sofisticados e complicados modelos de risco tal como admiram os modelos comerciais de negócio, por exemplo? Como é que os fundamentos de seu atual programa de segurança podem competir com métricas orientadas ao negócio?

### **Respostas:**

Os executivos de negócio têm de acreditar e confiar em você, e você só vai ganhar

essa credibilidade fazendo aquilo que se comprometeu a fazer para proteger a informação deles. Se você cometer erros, será descoberto em pouco tempo (tal como seu antecessor foi), mas se fizer a coisa certa ganhará a credibilidade de seus gestores, poderá melhorar seu conjunto de métricas para apontar os riscos realmente importantes para o negócio e não apenas indicadores para serem apresentados.

Lembre-se, tudo é baseado em credibilidade. Credibilidade se constrói com qualidade de serviço, não com quantidade de indicadores.

**André Pitkowski**

Consultor na área de Governança, Risco e Compliance.

sumário

# Responsabilidades sobre a Conexão Wireless

*Camilla do Vale Jimene e Renato Opice Blum*

Nos dias atuais, é fato que a tecnologia está amplamente inserida em nosso cotidiano, porém, algumas vezes, esquecemos o impacto que esse aparato tecnológico pode causar na esfera jurídica.

Um dos temas bastante discutidos recentemente pelos Tribunais em âmbito mundial são as responsabilidades dos usuários sobre a utilização das conexões sem fio à Internet.

Na Índia, terroristas utilizaram as conexões sem fio desprotegidas para enviar ameaças, já na Inglaterra, um homem desempregado foi preso por uso não autorizado da conexão wireless do vizinho. No Brasil, a praia de Copacabana já oferece rede sem fio em toda a sua orla gratuitamente, enquanto nos EUA, as cidades de Chicago e Baltimore vêm exigindo cadastro dos seus usuários wireless.

É certo que existem inúmeros motivos para o usuário optar por utilizar uma rede sem fio de acesso à Internet, porém aquele que não restringe o acesso por meio de senha ou criptografia e tem sua conexão utilizada para práticas ilícitas, por alguém totalmente desconhecido, pode ser responsabilizado?

Em recente decisão, o Tribunal de Justiça do Estado de São Paulo enfrentou essa questão e condenou uma empresa do tipo lan house ao pagamento de indenização por danos morais, por não ter conseguido identificar o usuário de sua conexão sem fio que enviou mensagem eletrônica anônima com teor ofensivo à vítima.

A decisão foi embasada em uma lei estadual paulista que prevê a obrigação do estabelecimento manter cadastro atualizado dos usuários, porém os julgadores também discorreram acerca dos riscos da utilização indiscriminada da conexão wireless.

Os desembargadores do Tribunal Paulista entenderam que a atividade de fornecimento de acesso à Internet a um número grande de pessoas, seja ele por meio de rede sem fio ou por meio de cabo, possibilita riscos efetivos aos direitos de terceiros, caso não sejam tomadas as precauções necessárias, especialmente o cadastramento dos usuários

que permita identificar a autoria de eventual ilícito cometido.

De fato, essa decisão também poderá gerar reflexos no âmbito corporativo, pois são muitas as companhias que migraram suas conexões para redes sem fio, de olho no futuro, mas sem considerar os riscos legais que podem envolver a utilização dessa tecnologia.

Essa questão é recente e ainda vai causar muita polêmica no Brasil e no mundo, especialmente quanto à obrigatoriedade ou não da adoção de cautelas de ordem técnica na utilização de qualquer nova tecnologia, seja para evitar a utilização indevida, seja para ter argumentos de defesa em caso de ato ilícito. Afinal, sempre é melhor prevenir do que remediar!

**Renato Opice Blum:**

Advogado e economista. Coordenador do curso de MBA em Direito Eletrônico da Escola Paulista de Direito.

**Dra. Camilla do Vale Jimene**

Advogada associada à Opice Blum Advogados e Professora de Direito Eletrônico em diversas instituições.

sumário)



## **Sua empresa está preparada para um evento de DESCONTINUIDADE??**

A operacionalização de um PCN é um processo estruturado para:

- Melhorar proativamente a resiliência da empresa contra possíveis descontinuidade;
- Restabelecer a capacidade de fornecimento de produtos e serviços;
- Proteger marca e reputação

O PCN possui normatizações e regulações, com base nas melhores práticas internacionais.

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

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

## **Consulte – nos!!!!**



# A importância do embasamento metodológico no ensino especializado

Álvaro Takei

Capacitar adultos é bem diferente de ensinar crianças e adolescentes.

Os professores e instrutores sabem que uma atenção especial deve ser dada ao método de aulas. Normalmente, se valem de conhecimentos baseados na própria experiência, de características pessoais e de técnicas aprendidas, o que acaba se tornando um modelo particular. Nessa linha de raciocínio, alguns obtêm sucesso outros não.

De qualquer forma, sempre há uma técnica didática adotada, em alguns casos até sem saber que se segue um modelo. Um grande número empresas de treinamento, bem como, de escolas de nível superior voltadas, portanto, para a educação de adultos, vêm usando as mesmas técnicas didáticas utilizadas no ensino médio e no fundamental, quer dizer, aplicam a pedagogia, sem atentar que a origem da palavra (do grego “*paidós*”, que significa criança) já indica que a técnica não se aplica a adultos.

No ensino fundamental lidamos com sujeitos que, por força da necessidade de serem alimentados, vestidos, protegidos, em suma amparados em todos os aspectos, possuem uma

dependência em relação às pessoas próximas, notadamente, pais e parentes. Esta dependência estende-se à escola, onde, então, a autoridade e a orientação dos professores são inquestionáveis.

A situação de dependência da infância, na adolescência, vai modificando para uma situação de questionamento, surgem as rebeldias e, aquilo que era inquestionável, passa a ser visto como algo falível. Assim, nesta fase, na escola começam a querer saber qual a razão de terem de aprender diversas disciplinas.

Na fase adulta temos o sujeito independente. O indivíduo está acumulando experiências, aprendendo com os próprios erros e se conscientizando dos assuntos que desconhece e o quanto essa ignorância é prejudicial. Dessa forma, possui a habilidade de analisar e criticar cada informação que recebe, no mínimo, classificando-a como útil ou inútil.

Logo, ignorar essa evolução pode levar a erros nos sistemas tradicionais de ensino. Torna-se, então, importante atentar para o crescimento do indivíduo e aplicar a didática apropriada para cada fase. Nesse sentido, vale a pena pensar se a Andragogia, aliada à Tecnologia da Informação, é indicada, como mais um subsídio para a educação de adultos, em consequência, compor o modelo a ser aplicado nos cursos e treinamentos.

## CONCEITOS

Andragogia é uma Ciência que estuda como o adulto aprende, sua característica principal é eliminar a resistência às mudanças, preparando o indivíduo a novas idéias e ao novo aprendizado, ou seja, provocando mudança interna de cada indivíduo.

Segundo Knowles, é uma tentativa para desenvolver uma teoria específica para o aprendizado relacionado a pessoas adultas. Knowles enfatiza que adultos são autodirecionados e esperam ter responsabilidade na tomada de decisões. Os programas de aprendizado adulto precisam se adaptar a esse aspecto fundamental.

A Andragogia atenta sobre a importância do conteúdo selecionado para adultos, porém, a maior ênfase é dada aos cuidados que o método de ensino deve conter para favorecer a efetiva aprendizagem.

O objeto da educação de adultos não é tanto ministrar o ensino, mas assegurar uma formação. Ele visa criar um clima de curiosidade intelectual, de liberdade social e de tolerância e suscitar, em cada um, a necessidade e a possibilidade de participar ativamente no desenvolvimento da vida cultural de sua época. A Andragogia se aplica a qualquer forma de aprendizado para adultos e tem sido extensivamente usada no modelo de programas de treinamentos organizacionais, de algumas empresas e consultorias, dentre elas a Brasileiro & Associados.

## PREMISSAS

A Andragogia possui algumas premissas, considerando que o adulto é sujeito da educação e não objeto dela, as principais são as de que os adultos:



1. precisam saber porque têm de aprender algo;
2. precisam aprender experimentalmente;
3. abordam o aprendizado como resolução de problemas;
4. aprendem melhor quando o tópico é de valor imediato;
5. possuem consciência de que necessitam adquirir conhecimentos;
6. possuem capacidade para o autodesenvolvimento;
7. está pronto para aprender o que decide aprender.



Portanto, de forma sucinta, significa que a instrução para adultos precisa focalizar mais o processo e menos o conteúdo que está sendo ensinado. Estratégias, como estudos de casos, encenações, simulações e auto-avaliação são muito úteis. Os instrutores adotam um papel de facilitador ou fonte, em vez de mero conferencista.

## PRINCÍPIOS

O processo de aprendizagem do adulto se desenvolve segundo uma seqüência:

- a) Sensibilização – recebidos os estímulos necessários surge a motivação;
- b) Estudo – explicações recebidas, pesquisas, trabalhos etc.;
- c) Discussão – esclarecimento;
- d) Experimentação – prática;
- e) Conclusão – convergência;
- f) Compartilhamento – sedimentação.

Considerando a seqüência de aprendizado e que o adulto é um indivíduo maduro para assumir responsabilidades por seus

atos perante a sociedade, bem como as premissas andragógicas, passamos a elencar alguns princípios que devem ser levados em conta para o sucesso na educação de adultos:

1. Existe a necessidade de explicar porque coisas específicas estão sendo ensinadas;
2. A instrução precisa ser orientada para o trabalho, em vez de ser direcionada para a memorização - as atividades de aprendizado devem estar no contexto de tarefas comuns a serem realizadas;
3. A instrução deve considerar a grande faixa de diferentes *backgrounds* dos aprendizes; os materiais e as atividades de aprendizado devem levar em conta que existem diferentes níveis e tipos de experiência anterior de cada participante;
4. Como adultos são autodirecionados, a instrução deve permitir que aprendizes descubram as coisas por si só, fornecendo orientação e ajuda quando erros são cometidos;



5. Adultos precisam estar envolvidos no planejamento e avaliação de suas instruções;
6. Experiência (inclusive erros), principalmente de forma compartilhada, fornece a base para as atividades de aprendizado;
7. Adultos são mais interessados em aprender matérias que têm relevância imediata para seu trabalho ou vida pessoal;
8. O aprendizado adulto é centralizado no problema, em vez de ser orientado para o conteúdo;
9. O adulto é dotado de consciência crítica;
10. A relação educacional é fundamentada na interação entre facilitador e aprendiz, num clima de liberdade e pró-ação;
11. Necessidade de liberdade de expressão e participação;
12. A educação de adultos é baseada na reflexão e ação, onde os assuntos são discutidos e vivenciados.

## CONCLUSÃO

A Andragogia leva à conclusão da existência de articulações entre a educação de adultos e W profissional. Apresentada em contraposição à pedagogia, a andragogia, tal como entendida por diversos autores, superaria as limitações da primeira. Conclui-se, também, que adultos esperam estar o mais próximo possível da área de aplicação dos conhecimentos que irá adquirir, objetivo que pode ser alcançado com ferramentas de ensino a distância.

Dessa forma, você leitor, ao fazer a escolha por um curso ou treinamento deve verificar se a organização ministrante possui o conhecimento de técnicas de ensino adulto,

por exemplo, a Andragogia aqui tratada, assim como, se domina tecnologias que permitam a educação à distância.

Há um enfoque democrático na proposta, que deve fazer parte do processo formativo dos adultos. Deve existir flexibilidade, tanto para que possam participar de treinamentos, quanto para que se realizem mudanças de percurso que estejam de acordo com demandas e aspirações dos educandos.

O estudo da Andragogia deixa clara a necessidade de revisão de técnicas e conceitos didáticos e enfatizam que o ensino deve ser levado onde os aprendizes estão, tais conceitos e técnicas têm sido adotados em diversos cursos destinados a educação de adultos, notadamente na Brasileiro & Associados, cujos treinamentos estão fortemente calcados em técnicas e exemplos pragmáticos, onde os instrutores são, antes de tudo, profissionais nos assuntos ensinados, somada à forte utilização da tecnologia da informação nos cursos a distância.

## REFERÊNCIAS

KNOWLES, M.. **Andragogy in Action**. San Francisco: Jossey-Bass, 1984.

KNOWLES, M.. **Self-Directed Learning**. Chicago: Follet, 1975.

KNOWLES, M.. **The Adult Learner: A Neglected Species** (3rd Ed.). Houston, TX: Gulf Publishing, 1984.

\* Texto original do autor

**Álvaro Takei**

Diretor de Ensino Digital da Brasileiro & Associados

takei@brasiliano.com.br

*sumário*

 **treinamento**

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

## PREPARE-SE !! FAÇA DIFERENÇA !!

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

informações | 11 5531-6171  
| [www.brasiliano.com.br](http://www.brasiliano.com.br)  
| [info@brasiliano.com.br](mailto:info@brasiliano.com.br)

 **b&a**  
BRASILIANO & ASSOCIADOS



## A COLEÇÃO QUE FALTAVA AO MERCADO DE GR

A Sicurezza Editora está lançando no próximo mês de novembro a Coleção Gestão de Riscos. São 50 títulos abordando temas como: Sistemas de Informação, Incêndio, Investigação, Segurança Pessoal, Segurança Patrimonial, GRC, Inteligência e Gestão Pura.

A cada mês, serão lançados de dois a três livros inéditos na área de Gestão de Riscos Corporativos.

Segundo Antonio Brasiliano, a intenção do lançamento é a de suprir a insuficiência de biografia de sistemas de segurança, completando “uma lacuna no mercado de risco e segurança”.

Na primeira semana de novembro serão lançados os títulos **Análise de Risco Corporativo-Método Brasileiro Avançado** e **As Formas do Crime** de Tulio Kahn. E para festejar os lançamentos será realizada uma noite de autógrafos em breve. Confira nosso blog para saber a data e o local do evento.

## O MÉTODO ESSENCIAL DA GR ALINHADO COM A ISO

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

O novo método de Antonio Celso Ribeiro Brasiliano é a nova bíblia dos gestores de risco, pois retoma e aprofunda a famosa metodologia para aqueles que já dominam as diretrizes básicas da gestão de riscos nas empresas.

*Gestão e Análise de Riscos Corporativos – Método Brasileiro Avançado de Análise de Riscos* (Sicurezza Editora, 2009) traz uma explanação aprofundada da nova norma internacional de gestão de riscos, a ISO 31000.

O livro “tem a finalidade de ajudar os gestores de riscos a implantarem um processo lógico de gestão e análise de riscos, possuindo critérios, métodos e ferramentas que já são utilizadas em inúmeras empresas no Brasil e no mundo”, conforme acentua Brasiliano.



O Método Brasileiro Avançado fornece um processo para a identificação dos perigos, avaliação dos seus Fatores de Riscos, análise e avaliação dos riscos corporativos, ao longo de 13 capítulos essenciais.

Além da definição e aplicabilidade da norma ISO 31000, a obra também dissecou normas já conhecidas como a metodologia COSO e a ISO Guia 73.

Como ferramenta nova, foi incluso no livro a Matriz de Impacto Cruzado, para poder verificar o nível de motricidade dos Fatores de Risco. Também foi adicionado ao novo método o Plano de Ação, para poder ter uma priorização de ações. Segundo o autor, foram colocados “indicadores para que o gestor possa tomar suas decisões pensando ‘qual ação é prioritária frente a uma relação custo x benefício’”.

A compreensão do método torna-se total aos leitores dedicados que terão a possibilidade de aplicar todo o conhecimento embasado em experiência de mais de 20 anos do autor na área de Gestão de Riscos Corporativos.

## DO EFEITO SE CHEGA À CAUSA

*O sociólogo, cientista político e criminólogo Tulio Kahn, relança pela Sicurezza Editora o livro As Formas do Crime, um verdadeiro manual prático*

Insegurança e violência são temas exaustivamente debatidos e pouco solucionados no Brasil. Entender as razões dos atos criminosos a fim de secar a fonte da atitude delituosa, é dever não apenas dos responsáveis pela gerência da segurança pública mas também de todos os homens e mulheres, já que o ímpeto surge na natureza humana e é estimulado ou controlado pela sociedade dos homens.

Com extensa experiência na área de segurança, ninguém melhor do que Tulio Kahn para dissecar todas as maneiras que os atos ilícitos possam se manifestar.

Em sua carreira pública, iniciou-se em 1999 como assessor na Secretaria da Administração Penitenciária. Em 2002, foi Coordenador de Pesquisa do Ilanud. No Ministério da Justiça, atuou em 2003 como Diretor do Decasp e na Secretaria de Segurança Pública, trabalhou como coordenador de análise e planejamento.

Internacionalmente, Kahn foi vice-chairperson do encontro da ONU em Viena, de 8 a 10 de fevereiro de 2006 para estudar formas de



aprimorar a coleta de dados criminais para atender as novas convenções sobre corrupção e crime organizado transnacional e sugerir indicadores que fossem simples e universalmente compreendidos para estimar a extensão do crime organizado no mundo a fim de monitorá-lo e propor medidas para combatê-lo.

Por toda essa bagagem, com a qual lhe foi possível aprender a administrar a aplicabilidade de recursos escassos em necessidades crescentes, o pesquisador denota em sua obra uma preocupação eminentemente prática.

Mas por que as qualificações ante os motivos? Como o próprio Kahn explica, “as formas em que um fenômeno criminal se manifesta nos dão pistas importantes para a interpretação correta do que o provoca, ajudando a eliminar as correlações espúrias”.

O mestre e doutor em Ciência Política pela USP, explica a razão do estudo, quando diz que esses “não nos auxilia apenas no esforço interpretativo, preocupação dos estudiosos do tema, mas também a estabelecer políticas públicas concretas para lidar com ele – independentemente de termos ou não esclarecido suas causas fundamentais.” Ele explica, dizendo que “se sabemos que os homicídios, por exemplo, concentram-se nas noites dos finais de semana e que resíduos de álcool são freqüentemente encontrados nas vítimas, é possível pensar em políticas públicas como a “Lei Seca” ou a “Noite das Mulheres” – apenas com base no conhecimento deste perfil epidemiológico.”

Os artigos que compõem a obra são de caráter essencialmente descritivos e pouco interpretativos, dada a finalidade a que almejam: a utilidade prática.

Embasadas em indicadores adequados e com análises objetivas e imparciais, a obra deve ser livro de cabeceira a todos os profissionais da área ou aficionados em Criminologia.

As formas do crime por quem possui e para quem procura teoria e prática.

sumário