b&a BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

março 2009 | edição 41

FRAUDE

Gerenciando Riscos de Fraude através da sua Lógica

EM FOCO

Auditoria de Riscos: Novo Enfoque

SEGURANÇA DA INFORMAÇÃO

Gestão de Riscos Corporativos e Ferramenta de TI Audixpress

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

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

Colunistas | Álvaro Takei, Mariana Fernandez e Ricargo Yagi. **Colaboradores desta edição** | Fernando de Bonneval de Carvalho, Gustavo Cirelli, Joffre Coelho Júnior, Rosangela Aparecida Stringher, Sandra Alves e Silvia Ferreira Netto

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

PONTO DE VISTA

Auto Avaliação de Riscos e Controles – AARC, você conhece??

A crise do sistema financeiro mundial faz com que tenhamos, obrigatoriamente, na gestão de nossas áreas de negócio, criatividade e visão prospectiva!

A Auto Avaliação de Riscos e Controles, chamada de AARC, é uma metodologia que faz com que toda a empresa esteja comprometida com a Gestão e Controle dos Riscos Corporativos. O comprometimento dos usuários faz com que a empresa e seus respectivos processos de negócios possuam níveis de riscos aceitáveis, além de poder gerenciá-los.

A AARC consiste uma metodologia iniciada na empresa petrolífera GULF – Canadá, em 1987, para atender a um decreto local, sendo inicialmente utilizada por Auditores Internos que necessitavam de novas abordagens no exame da efetividade dos controles internos. Trata-se de metodologia utilizada para avaliação e revisão dos principais objetivos dos negócios da organização, dos riscos envolvidos na busca por atingir esses objetivos e dos controles internos projetados para administrar esses riscos, avaliando a sua eficácia. É uma metodologia que pode ser utilizada tanto pelo gestor quanto pelo auditor, para avaliar a adequação dos processos de gestão de riscos e controles da empresa.

A AARC facilita a coleta e a transmissão da informação, promovendo melhorias na gestão de riscos e controle, encorajando o compartilhamento e a colaboração e auxiliando a empresa na criação de uma cultura mais aberta e compartilhada. Como valor mais importante, a Auto Avaliação de Riscos e Controles tem o auxílio direto no cumprimento dos objetivos da empresa.

Além de metodologia a AARC é também um processo, através do qual a eficácia do controle interno é examinada e avaliada. Seu objetivo é o de prover uma segurança razoável, de forma que todos os objetivos de negócio sejam alcançados.

Um programa eficaz de AARC deve aumentar a cobertura da avaliação de riscos e processos de controle, melhorar a qualidade das ações corretivas feitas pelos proprietários do processo e focalizar o trabalho da auditoria sobre a revisão dos processos de alto risco e situações anormais.

A crença da AARC tem como base a confiança de que o pessoal que de fato executa a função tem profundo conhecimento do processo, incluindo seus pontos fortes e deficiências no ambiente de risco e controle. Tal pensamento leva à otimização de recursos humanos e capilarizarização da cultura de riscos e controles.

O fator Chave de Sucesso na operacionalização da AARC é o Fator Humano. A empresa deve assegurar que todos os participantes estejam cientes e adotem os conceitos de Controle de Riscos. Deve também assegurar que o pessoal possua consciência de seus papéis e responsabilidades, da política e procedimentos da empresa, e conhecimento em controles.

O Fator Pessoa – não a tecnologia ou procedimentos de controle – é um fator chave para prover um nível apropriado e adequado de controle e responsabilidade. Se as pessoas são chaves, são também o elo mais fraco, portanto deve-se sensibilizá-las. Uma conscientização robusta é primordial para que as pessoas compreendam o contexto organizacional.

Este, senhores, é mais um novo desafio para nós gestores de riscos e auditoria, pois desta forma podemos enxugar nossas estruturas mantendo-as constantemente monitoradas e gerenciadas. Os benefícios hoje são plenamente mensuráveis, entre eles podemos citar a monitoração contínua das atividades, antecipação, fatores de riscos inseridos hoje nos planos de auditoria e revisão antecipada.

Espero que consigam quebrar este paradigma e otimizem recursos nestes nossos tempos bicudos.

Sorte e sucesso a todos!!

Antonio Celso Ribeiro Brasiliano
Diretor Executivo
abrasiliano@brasiliano.com.br

b&a
BRASILIANO & ASSOCIADOS

EDITORIAL

Gestão de Riscos:
Conteúdo Técnico e Antenado

Conforme anunciado na edição anterior, nas páginas seguintes você vai conhecer a nova revista da Brasiliano & Associados: Gestão de Riscos.

Com páginas interativas, você irá se aprofundar em artigos técnicos escritos pelos consultores da B&A, navegando pelos assuntos do mundo dos negócios envolvendo riscos corporativos.

Nesta edição você irá saber Como terceirizar serviços de segurança, através do artigo da Técnica de Segurança Patrimonial Silvia Ferreira Netto, na seção Outsourcing.

O publisher da Gestão de Riscos, Antonio Brasiliano, aborda fraudes nesta edição, e destaca as ações preventivas que podem ser tomadas contra os fraudadores.

Em Segurança da Informação, o consultor Fernando de Bonneval de Carvalho, fala sobre as necessidades da Gestão de riscos empresariais e a ferramenta de auditoria AudiXpress, aderente às principais normas de riscos.

A necessidade de um PCN (Plano de Continuidade de Negócios) quando da ocorrência de algum impacto negativo nos negócios já é conhecida por muitos, mas, na seção Análise, a consultora Sandra Alves, Especialista em Gestão da Segurança Empresarial, destaca Os maiores erros da empresas no planejamento da continuidade de negócios.

Rosângela Aparecida Stringher, também traz novidades na área de auditoria na seção Em Foco; explicando o novo enfoque da auditoria de riscos atual.

Na seção Gestão de Riscos, Gustavo Cirelli, faz uma abordagem mais conceitual explanando a Aplicação do diagrama de causa e efeito no processo de análise de riscos.

O cordenador técnico dos cursos da B&A, Joffre Coelho Chagas Jr., nos brinda com um artigo sobre a ação de Desinformação promovida pelo serviço de Inteligência das empresas.

As colunas estão super interessantes. Em tecnologia, o engenheiro Ricardo Yagi traz uma visão geral sobre o CFTV (Circuito Fechado de Televisão), abrangendo os pontos fortes e limitações de cada tipo tecnológico.

Em treinamento, o Prof. Álvaro Takei, Diretor de Ensino Digital da B&A, explica o papel do auditor líder em gestão de riscos e na coluna Ler & Saber, você fica por dentro de dois grandes lançamentos sobre riscos digitais e a importância da ousadia na gestão empresarial.

Use e abuse dos links e botões para deleitar-se na leitura de um conteúdo comprometido com a busca de soluções inteligentes na gestão de riscos.

Boa leitura!
Mariana Fernandez

b&a
BRASILIANO & ASSOCIADOS

Você sabe o TAMANHO de seus RISCOS

A dimensão das conseqüências operacionais nem sempre são visíveis. Geram altos custos internos, falta de controle e uso inadequado de sistemas e equipamentos, fazendo com que a empresa perca sua competitividade.

b&a
BRASILIANO&ASSOCIADOS

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

A BRASILIANO & ASSOCIADOS analisa e avalia seus riscos, otimiza processos e oferece soluções completas para mitigação de riscos. Com a BRASILIANO & ASSOCIADOS sua empresa terá uma nova visão de negócios.

Os Maiores Erros das Empresas no Planejamento da Continuidade de Negócios

Sandra Alves

Vivemos em um mundo ameaçado por inúmeros incidentes, que podem ser causados por mudanças econômicas, ambientais, sociais, tecnológicas etc, colocando a estabilidade dos negócios em risco. Sobreviver aos danos provocados por impactos de eventos inesperados de ruptura é a principal razão para que qualquer empresa implemente o Plano de Continuidade de Negócios.

O que avaliamos é que não são poucas as empresas que julgam desnecessário contratar um serviço de PCN (Plano de Continuidade de Negócios), principalmente porque demanda tempo (cultura e estruturação do plano) e investimento. Porém, quando acontece o incidente (crise), que provoca impacto diretamente na imagem, no financeiro, na legislação e até no operacional de uma empresa, estima-se um problema incalculável.

Podemos definir 'Plano de Continuidade de Negócios' (PCN) como o planejamento e a realização de ações que têm como objetivo assegurar a continuidade das operações dos processos de negócio da empresa, na eventualidade de uma indisponibilidade prolongada dos recursos que dão suporte à realização dessas operações (equipamentos, sistemas de informação, instalações, pessoal e informações).

No ano passado, uma pesquisa realizada pela Aon com 320 executivos de diversos segmentos, em 29 países, revelou que o risco mais temido pelas grandes corporações é relativo aos danos à reputação da empresa. Ele é encarado como a maior fonte de vantagem competitiva.

O estudo traz uma fotografia dos riscos empresariais e o quanto eles são parecidos, independentemente do setor de atuação.

O segundo risco potencial citado pelos executivos na pesquisa foi a interrupção de negócios, para o qual 30% dos entrevistados disseram que a empresa não está preparada para enfrentar o problema. O terceiro maior risco comentado pelos profissionais entrevistados foi o de responsabilidade civil, potencializado pela globalização e influência de culturas mais litigiosas, como nos Estados Unidos, onde processar virou um hábito.

Para estabelecer processo, princípios e a terminologia da Gestão de Continuidade de Negócios (GCN), a Associação Brasileira de Normas Técnicas (ABNT) lançou a norma 15999-1: Código de prática, e 15999-2: Requisitos.

O propósito da norma 15999:1 é estimular as empresas para adoção das melhores práticas em GCN, orientando a criação de planos de respostas a incidentes, para fornecer uma base que propicie o entendimento, o desenvolvimento e a implementação do tema.

A norma 'Gestão de Continuidade de Negócios' (GCN) é um processo da organização que estabelece uma estrutura estratégica e operacional adequada para:

- Melhorar proativamente a resiliência da organização contra possíveis interrupções;
- Prover uma prática para restabelecer a capacidade de fornecimento de produtos e serviços;
- Obter reconhecida capacidade de gerenciar uma interrupção no negócio, protegendo marca e reputação.
- O ciclo de vida GCN é composto por seis elementos, que podem ser visualizados na figura 1. Estes podem ser implementados em organizações de todos os tamanhos, em todos os setores: públicos, privados, sem fins lucrativos, educacional, manufatura etc.

Figura 1 – Ciclo de Vida da GCN

A Gestão de Continuidade de Negócios é um elemento importante à boa gestão de negócios, fornecimento de serviços e prudência empresarial.

Os gestores e proprietários têm a responsabilidade de manter a capacidade de funcionamento, sem interrupção da organização. As organizações constantemente assumem compromissos ou têm o dever de entregar os produtos e serviços; ou seja, assinam contratos e criam expectativas. Todas as organizações têm responsabilidades morais e sociais, principalmente nos casos em que elas forneçam uma resposta de emergência ou um serviço público ou

voluntário. Em alguns casos, as organizações têm obrigações legais ou regulamentares de efetuar um GCN.

Um planejamento de continuidade dos negócios bem definido, estruturado, testado e divulgado aos colaboradores pode ajudar uma empresa a economizar milhões de reais, evitando assim a perda de negócios, fortalecendo a marca e aprimorando, de forma geral, a vantagem competitiva.

Infelizmente, a maioria dos planos de continuidade existentes nas empresas é feito 'só para inglês ver'. Cumpre-se apenas uma normativa da empresa em um momento de 'contingência'. Percebe-se que isso acontece quando realmente a crise chega e os colaboradores não sabem o que fazer e como fazer.

A principal causa de fracasso na elaboração de planos de continuidade de negócios é decorrente da falta de apoio da alta direção, de restrições orçamentárias, sensibilização/comprometimento dos colaboradores e também a não aplicação de testes, ou seja, simulações em casos de crise.

É importante refletir sobre alguns aspectos, para que em um momento de 'contingência', não sejamos surpreendidos. Quais riscos a empresa tem? Quais os riscos de maior probabilidade e maior impacto no negócio da empresa? Você sabe a quem se reportar em caso de incidente? Qual a estratégia em caso de 'contingência'? Quais são os processos críticos de uma empresa e quanto tempo eles suportam ficar parados? O plano de continuidade de negócio está focado em TI ou visa todos os de processos de negócios da empresa? O PCN da sua empresa está atualizado e testado?

O planejamento de continuidade de negócios pode parecer algo caro e demorado. Porém, paralisar os processos de negócios, funções, sistemas, a própria empresa e seus clientes pode ser devastador. Construa seu plano, treine, teste, treine e teste novamente, destacando como ponto crucial a sensibilização e o comprometimento dos seus colaboradores sobre a importância do PCN na empresa.

Referências

ABNT NBR 15999- 1: Gestão de continuidade de negócios – Parte 1: Código de Pratica

Sandra Alves
Consultora da Brasiliano & Associados
salves@brasiliano.com.br

sumário

Como Terceirizar Serviços de Segurança

Silvia Ferreira Netto

Atualmente, o que encontramos no mercado são empresas com necessidades de reduzir seus custos. Mas quando tratamos de serviços, esta redução deve chegar até um limite onde não ultrapasse a razão da existência de uma empresa, ou seja, a sua prosperidade, obtida através da manutenção da integridade de seus contratos. Isso se dará somente se a contratada tiver condições de honrar seus compromissos sociais, tributários e financeiros e, ainda, proporcionar crescimento para seus colaboradores.

Hoje, existe uma grande campanha contra a clandestinidade, mas precisamos mais que isso. Há necessidade de conscientização por parte do mercado como um todo para os preços. O que hoje pode parecer 'barato' amanhã pode custar muito caro, tendo em vista que, no caso da extinção da prestadora, todo o passivo trabalhista passa ser de responsabilidade direta da contratante.

Nos últimos anos, muitas prestadoras deixaram de existir. Elas adotaram políticas de preços inexequíveis para atender ao mercado, além do passivo trabalhista, que fica sob encargo da contratante. Assim, muitos funcionários foram lesados moral e financeiramente.

O cuidado ao contratar as prestadoras vai além da legalidade. A contratante deve ter como requisito a forma de gestão da prestadora, ou seja, como são geridos os recursos humanos,

financeiros e operacionais. Dentro desta perspectiva, podemos perceber que a documentação da empresa demonstra como são honrados os seus compromissos, já a referência dos seus clientes, fornecedores e colaboradores refletem a qualidade do seu atendimento. As planilhas abertas, não menos importantes, evidenciam como é a política de formação de preço, se a legislação é respeitada e se todos os encargos e insumos estão sendo contemplados. Empresas éticas são responsáveis e não deixam de cumprir com todas as suas obrigações trabalhistas, tributárias e sociais.

Outro ponto a salientar é que as contratantes devem deixar claro nesta contratação o que esperam obter: apenas a mão de obra ou a segurança? No primeiro caso, é importante a presença no seu quadro funcional de um gestor de segurança com conhecimento na área, pois será este quem definirá as diretrizes e o escopo dos serviços. Ele será o responsável pela implantação, acompanhamento e avaliação da equipe, não cabendo aqui responsabilizar a prestadora pelos erros causados por decisões equivocadas, que provoquem algum tipo de dano às pessoas ou ao patrimônio da contratante. Quando se terceiriza a segurança de fato, a prestadora assume toda essa responsabilidade. Assim, quem tomar para si esta gestão, deve estar capacitado para analisar, tratar e/ou administrar os riscos existentes.

Para facilitar o processo de contratação dos serviços de segurança e torná-lo mais prático e eficiente, seguem algumas dicas:

Iª FASE: LEGALIDADE QUANTO AO FUNCIONAMENTO

Quando uma empresa deseja terceirizar os seus serviços de segurança ou trocar de prestadora, deve tomar algumas precauções. A primeira delas é verificar se as selecionadas estão autorizadas a atuar no estado em que a Polícia Federal prestará o serviço. Antes de convidá-las a participar da concorrência, consulte o site do Sindesp, que disponibiliza a relação das empresas autorizadas. Lembre-se que, para cada estado, é necessária uma autorização específica. Ela não é válida para todo território nacional.

2ª FASE: HOMOLOGAÇÃO DAS PRESTADORAS

Sabendo quem está autorizada, antes do processo da concorrência propriamente dito, faça a homologação das participantes. Assim, evita-se perda de tempo em receber propostas de empresas que não estão com seus débitos sociais e tributários em dia ou daquelas que estão irregulares perante os órgãos pertinentes.

O contratante deve solicitar, nesta fase, a relação dos seguintes documentos:

- Certificado de Segurança - Ministério da Justiça (Departamento da Polícia Federal)
- Portaria de Autorização - Ministério da Justiça (Departamento da Polícia Federal)
- Alvará de Revisão - Ministério da Justiça (Departamento da Polícia Federal)
- Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União - Receita Federal

- Verificar autenticidade no site: www.receita.fazenda.gov.br
- Certidão Negativa de Débitos de Tributos Estaduais - Secretaria de Estado da Fazenda/PR Verificar autenticidade no site: www.fazenda.pr.gov.br
- Certidão Negativa de Tributos Municipais - Secretaria Municipal de Finanças da cidade onde a prestadora tem sede.
- Certificado de Regularidade do FGTS - Caixa Econômica Federal
- Verificar autenticidade no site: www.caixa.gov.br
- Certidão Negativa de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros - Ministério da Fazenda
- Verificar autenticidade no site: www.previdenciasocial.gov.br
- Guia de Recolhimento da Contribuição Sindical
- Solicitar informações ao Sindicato Patronal do Estado
- Certidão Negativa de Débitos Salariais e Trabalhistas - Ministério do Trabalho
- Atestado de Capacidade Técnica de alguns Clientes

Solicitar telefone de contato dos clientes para verificar a qualidade dos serviços

Todas as empresas que estiverem aptas, ou seja, apresentar todos os documentos válidos, serão chamadas para a terceira fase: Apresentação de Propostas Comerciais.

Importante: Atenção para a data de validade dos documentos e também para autenticidade das informações que estão disponíveis nos sites.

3ª FASE: PROPOSTAS COMERCIAIS

As propostas devem ser elaboradas com base num escopo bem claro e objetivo criado pelo gestor de segurança da contratante. Caso não exista esta função, chamar as participantes a realizarem uma visita técnica. O ideal é que todas sejam atendidas ao mesmo tempo, isso para garantir a imparcialidade de informações. Além de conhecer a unidade a ser atendida, devem apontar os seguintes dados:

- Escopo: quantidade de postos e suas funções (porteiro, vigilante, recepcionistas, etc.), escalas, carga horária, período e intervalos para refeições;
- Fornecimento de refeições: se a refeição é servida no local, informar o contato do fornecedor, o valor e horários de funcionamento do refeitório;
- Transporte: informar se há disponibilidade de utilização de ônibus

"Informar sobre a forma de pagamento e reajustes. Cabe salientar, neste caso, que é importante o repasse do dissídio na data base, pois aqui é que os valores podem ficar acima ou abaixo do mercado"

da empresa, contato do fornecedor e o valor;

- Se há necessidade de benefício adicional, como cesta básica, plano de saúde diferente do exigido em convenção, salários diferenciados ou outros;
- Informar se há necessidade de acessórios e/ou equipamentos como rádio, armamento, ronda eletrônica, sistemas de CFTV e alarme/pânico e outros;
- Informar se há necessidade de monitorar remotamente os sistemas eletrônicos;
- Informar sobre a forma de pagamento e reajustes. Cabe salientar, neste caso, que é importante o repasse do dissídio na data base, pois aqui é que os valores podem ficar acima ou abaixo do mercado. Importante priorizar a parceria, onde todas as partes ganham: contratante, contratada e funcionário;
- Informar sobre todos os itens que possam impactar em custo.

Um cuidado muito importante a ser verificado é em relação às atividades a serem realizadas, visto que apenas a vigilância armada ou desarmada tem regulamentação e autorização da Polícia Federal para exercer a função dentro dos limites do patrimônio da contratante. As demais funções são auxiliares. Com isso, o profissional pode apenas observar e não agir. São elas: Portaria, Recepção, Controle de Acesso, Vigia, etc.

Após a realização da visita técnica ou do envio do escopo dos serviços por parte do gestor de segurança, a contratante deve disponibilizar um e-mail para que as participantes possam enviar suas dúvidas, as quais devem ser respondidas rapidamente e de forma clara, com cópia para todas as demais concorrentes. Desta forma, o processo torna-se mais transparente e imparcial.

O tempo para entrega de propostas deve ser em média de 7 dias contados a partir da visita técnica ou do envio do escopo por parte do gestor de segurança. Assim, todas as participantes têm condições de elaborar uma proposta mais adequada à realidade da empresa.

Quando do recebimento das propostas, a contratante deve verificar as discrepâncias de preços, ou seja, ter a percepção dos exageros, tanto para cima como para baixo. Quando uma prestadora apresenta valores muito aquém da média, é preciso ter muita atenção e verificar se não está deixando de contemplar algum custo, o que pode gerar consequências indesejáveis para a contratante. Por exemplo: assumir um passivo trabalhista futuro, já que, legalmente, é um contrato de responsabilidade solidária e subsidiária.

Junto com a proposta comercial, sempre que possível, solicitar planilha de custos aberta para comparação. Interessante que seja individualizada por postos unitários para facilitar as verificações. Abaixo estão os itens que devem constar em tal planilha:

- Salários
- Adicional de Riscos
- Adicional de Intrajornada
- Adicional Noturno
- Adicional de Periculosidade ou Insalubridade (quando aplicável)
- Hora Reduzida
- Hora Extra
- Descanso Semanal Remunerado
- Encargos Sociais
- Vale Transporte
- Vale Alimentação

- Seguro de Vida
- Assistência Médica
- Uniformes / EPIs / Acessórios
- Armamento e Acessórios
- Treinamento e Reciclagem
- Sistemas de Comunicação
- Sistemas de Ronda
- Monitoramento de sistema eletrônico
- Outros equipamentos
- Taxa de Administração
- Taxa de Lucro
- Impostos (ISS, PIS, COFINS, IRPJ, CSSL)

No caso de a empresa ignorar algum custo, solicitar justificativas com bases legais e avaliar com muito critério.

4ª FASE: CONTRATAÇÃO DOS SERVIÇOS

Uma vez escolhida a prestadora, antes de anunciar a vencedora, é importante discutir todos os itens da proposta e certificar-se que esta terá condições de atender ao contrato de forma satisfatória e com a qualidade esperada. Ao elaborar o contrato, a contratante deve evidenciar todos os requisitos, prazos e forma de avaliação. Importante o envolvimento do jurídico para avaliar todas as cláusulas.

Depois da contratação, cabe a contratante monitorar e acompanhar não somente os serviços, mas também as obrigações trabalhistas, sociais e tributárias, verificando todos os meses, os seguintes documentos:

- Cópia do contracheque e comprovante de pagamento de cada trabalhador locado em suas dependências;
- Cópia da guia de recolhimento do INSS e do FGTS relacionadas aos trabalhadores locados em suas dependências;
- Cópia dos pagamentos de férias ou verbas rescisórias de todos os empregados que estejam ou estiveram locados em suas dependências, prestando serviços;
- Certificados, alvarás e certidões negativas de débitos atualizadas constantemente.

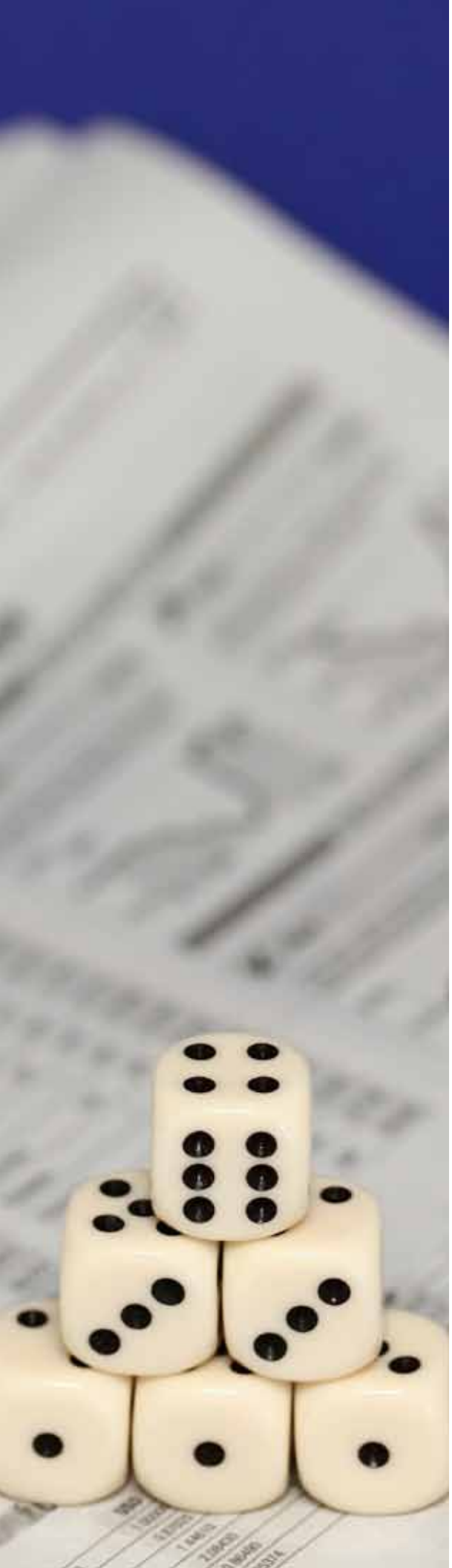
Todos os documentos devem ter suas cópias arquivadas mês a mês pelo tomador dos serviços, assim comprovando o cumprimento de todas as obrigações previdenciárias e trabalhistas.

Outra forma de acompanhamento é saber do próprio funcionário da prestadora a sua satisfação e verificar com o mesmo se este está sendo respeitado em seus direitos, com relação aos recebimentos. Também, a forma que se dá o atendimento e o tratamento por parte da mesma.

Ao acompanhar o desempenho da gestão de pessoas, operacional, administrativo e financeiro da prestadora, a contratante minimiza os riscos de problemas futuros. Lembrando que quando uma empresa não está bem financeiramente, o principal indício é o atraso no pagamento dos funcionários, assim como a entrega de vale alimentação, dos depósitos de fundo de garantia e dos recolhimentos do INSS.

Silvia Ferreira Netto
silviacferreira@hotmail.com

sumário



Auditoria de Riscos – Novo Enfoque

Rosângela Aparecida Stringher

A palavra 'auditoria' tem sua origem no latim, vem de 'audire', que significa 'ouvir'. É difícil precisar quando começa a história da auditoria, pois toda pessoa que possuía a função de verificar a legitimidade dos fatos econômico-financeiros, prestando contas a um superior, podia ser considerada como auditora.

Cronologicamente, há indícios da profissão desde o século XIV. Porém, o grande salto da auditoria ocorreu após a crise econômica americana de 1929. No início dos anos 30, foi criado o famoso Comitê May, um grupo de trabalho instituído com a finalidade de estabelecer regras para as empresas que tivessem suas ações cotadas na Bolsa, tornando obrigatória a auditória contábil independente nos demonstrativos financeiros dessas empresas.

Esses auditores independentes, no desenrolar de suas atividades, necessitavam ter acesso a informações e documentos que levassem ao conhecimento mais profundo e análises das diferentes contas e transações. Para tanto, funcionários da própria empresa foram designados. Estava lançada a semente da auditoria interna, pois os mesmos, com o decorrer do tempo, foram aprendendo e dominando as técnicas de auditoria, utilizando-as em trabalhos solicitados pela própria administração da empresa. Elas notaram que poderiam reduzir seus gastos com auditoria externa, se utilizassem melhor esses funcionários, criando um serviço de conferência e revisão interna, continua e permanente, a um custo mais reduzido. Os auditores externos também ganharam com isso, pois puderam se dedicar exclusivamente ao seu principal objetivo, que era o exame da situação econômico-financeira das empresas.

Após a fundação do The Institute of Internal Auditors, em Nova Iorque, a auditoria interna passou a ser vista de maneira diferente. De um corpo de funcionários de linha, quase sempre subordinados à contabilidade, pouco a pouco passaram a ter um enfoque de controle administrativo, cujo objetivo era avaliar a eficácia e a efetividade da aplicação dos controles

internos. O seu campo de ação funcional foi estendido para todas as áreas da empresa, e, para garantir sua total independência, passou a ter subordinação direta a alta administração da organização.

O termo risco provém do latim 'risicu' ou 'riscu', que significa 'ousar' (to dare, em inglês). Risco é a ameaça de que um novo evento afete a habilidade da empresa em atingir seus objetivos e suas estratégias de negócios, com potencial necessário de causar dano ao seu patrimônio, seja ele tangível ou intangível (BRASILIANO, Antônio Celso Ribeiro. Manual de Análise de Risco para a Segurança Empresarial. São Paulo: Sicurezza, 2003). De acordo com a Resolução CNS196/96, 'risco' é a possibilidade de danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente.

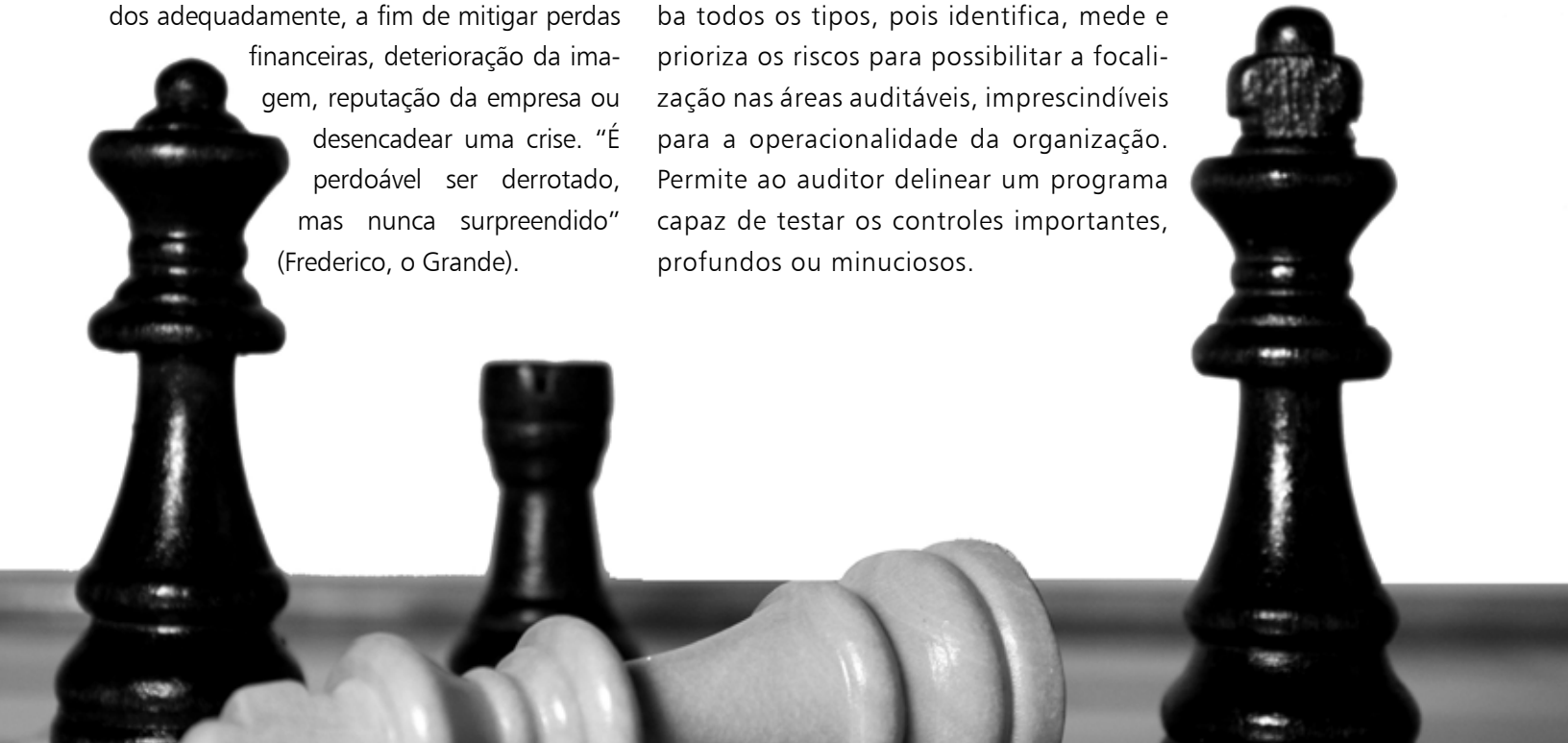
Todos os níveis das atividades do negócio estão suscetíveis a riscos, os quais podem diferenciar em função do ambiente empresarial, conforme o ramo em que a empresa atua. Podem estar relacionados à estratégia, finanças, tecnologia da informação, operação, conformidade e meio ambiente. Os riscos não podem ser temidos, mas enfrentados, monitorados e controlados. Por isso, necessitam ser gerenciados adequadamente, a fim de mitigar perdas financeiras, deterioração da imagem, reputação da empresa ou desencadear uma crise. "É perdoável ser derrotado, mas nunca surpreendido" (Frederico, o Grande).

O fato é que a garantia de continuidade dos negócios não se consiste em apenas recomendar e realizar controles internos, com base no histórico organizacional, a fim de tratar os riscos como era no passado. Atualmente, a capacidade de uma organização sobreviver em meio à competitividade imposta diariamente pela acelerada globalização de mercado, exige que a auditoria não se limite a controles, mas que mantenha o diferencial de agregar, ao conhecimento do histórico organizacional, um eficiente gerenciamento de riscos, que atenda todo o universo dos processos das áreas de negócios da companhia.

Na última década, embora algumas empresas ainda vejam a auditoria interna como despesa de controles de possíveis irregularidades, houve um "amadurecimento" no contexto empresarial e muitas empresas se conscientizaram de que adequar-se ao novo cenário é um desafio para os profissionais da área. Eles devem, inclusive, identificar controles obsoletos e/ou ineficazes, assim como é fundamental as empresas buscarem rentabilidade, diferencial competitivo e estratégias mais eficientes.

A avaliação de riscos em auditoria ou Auditoria Baseada em Riscos (ABR) engloba todos os tipos, pois identifica, mede e prioriza os riscos para possibilitar a focalização nas áreas auditáveis, imprescindíveis para a operacionalidade da organização. Permite ao auditor delinear um programa capaz de testar os controles importantes, profundos ou minuciosos.

"É perdoável ser derrotado, mas nunca surpreendido"



Um estudo realizado pelo Instituto de Auditores Internos (The Institute of Internal Auditors), dos Estados Unidos, concluiu que pelo menos um terço dos departamentos (equipes) e serviços de auditoria interna falha na utilização da ABR. Há indícios de que as razões possam ser diversas, como: incompreensão dos conceitos de risco; crença de que a avaliação dos riscos requer especializados conhecimentos e softwares; pouco tempo para o planejamento, devido ao ciclo contínuo das exigências de execução das auditorias; muitos serviços de auditoria interna sentem que a sua ação têm uma dimensão bastante reduzida para utilizar ferramentas de planejamento; os auditores internos sentem que não há harmonia das auditorias de conformidade legal, normativa e financeira com o risco.

Comparação entre o velho e o novo

Área de Auditoria	Velho Paradigma	Novo Paradigma
Foco da auditoria	Sistema de controles internos	Riscos do negócio
Foco dos testes	Atividades de controle	Atividades de tratamento de todos os riscos
Foco do relatório	Adequação e eficácia dos controles internos	Adequação e eficácia do tratamento dos riscos
Resultados da auditoria	Controles novos ou melhorados	Tratamento adequado dos riscos

Figura 1

A decisão em prevenir riscos futuros requer investimento financeiro para as organizações. O fato é que muitas, ainda, questionam se é válido ou não investir num projeto para algo que possa não ocorrer. A fim de esclarecer a questão, cabe lembrar que a proposta do novo enfoque da auditoria de riscos é de visão holística - prospectiva, ou seja, antecipatória às possíveis situações que definem uma estrutura operacional, que mitigue significativas perdas financeiras às organizações.

A Brasiliano & Associados, constantemente comprometida em oferecer serviços de extrema competência e qualidade, contempla, em sua metodologia, (figura 2) a Conjuntura Empresarial; Riscos Estratégicos – Identificação; Diagnóstico – Matriz Swot – Fofa; Técnicas de Análise de Riscos; Levantamento do Impacto Financeiro; Matriciamento de Riscos e Plano de Ação, e a mantém aplicável a todos os segmentos de mercado. "A metodologia Brasiliano foi desenvolvida com base na experiência em projetos de segurança e gestão de riscos. O conceito do planejamento em segurança é mensurar todo e qualquer perigo (real e/ou potencial)

que a empresa possui, e implantar medidas antecipatórias - preventivas, visando mitigar os possíveis impactos negativos na operação da empresa" (BRASILIANO, Antonio Celso Ribeiro. Análise de Risco Corporativo. São Paulo: Sicurezza, 2006).

Cabe ressaltar que a metodologia Brasiliano contempla as vigentes normas: Associação Brasileira de Normas Técnicas - ABNT ISO/IEC GUIA 73, Gestão de Riscos - Vocabulário - Recomendações para uso em normas; ABNT/CB-21, Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança; Risk Management - AS/NZS 4360:2004, Australian/New Zealand Standard, AS/NZS 4360, Gestão de Risco e HB 436:2004, Risk Management Guidelines Ompanion to AS/NZS 4360:2004. Projetou-se no esboço da ISSO FDS 31000, prevista para vigorar a partir de 30 de Junho de 2009.

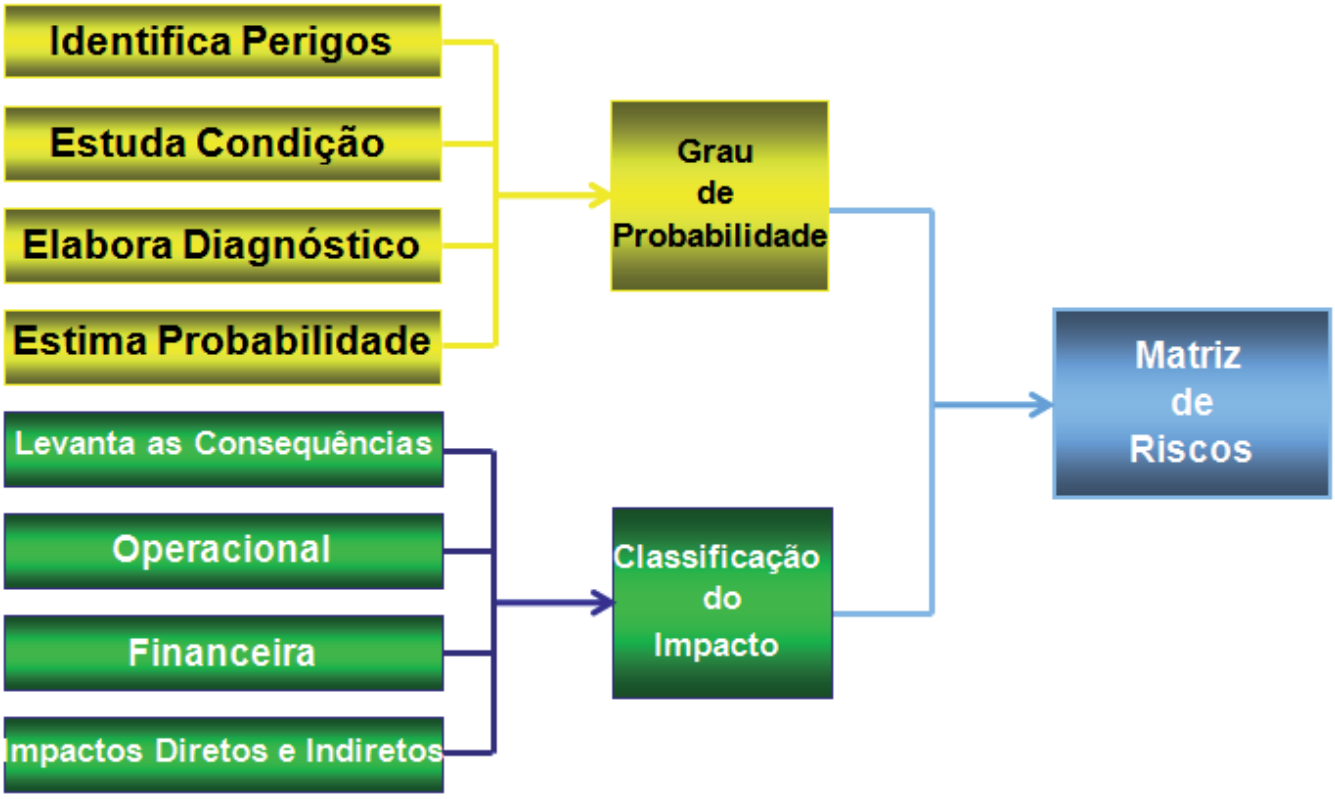


Figura 2

Fontes (Notícias e informações relacionadas):

(BRASILIANO, Antonio Celso Ribeiro. Análise de Risco Corporativo. São Paulo: Sicurezza, 2006)

(ATTIE, William. Auditoria Conceito e Aplicações.São Paulo: Editora Atlas, 1998 – 3ª edição)

http://www.cemla.org/pdf/aud-avalderisco.PDF

http://pt.wikipedia.org/wiki/Normas_brasileiras_de_auditoria

http://www.brasiliano.com.br/blog/?p=260

http://www.qsp.org.br/pdf/o_que_e_ABR.pdf

http://www.congressoeac.locaweb.com.br/artigos62006/432.pdf

http://www.ey.com/global/content.nsf/South_America_P/Servicos_-_Auditoria_-_Riscos_Financeiros

http://www.icbrasil.com.br

http://www.audicaixa.org.br/arquivos_auditoriaGerenciamentoRiscosCorporativos - IBGC.pdf

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

sumário

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!!!!

b&a
BRASILIANO&ASSOCIADOS

Sede Angola: | Rua Cirilo da Conceição e Silva, 22, primeiro andar Cj 07. Município das Ingombotas - Luanda - Angola
| Telefone Fixo: + 244 222 331 130 | Telemóvel: + 244 928 227 713 / + 244 924 868 614
| e-mail: riboldi@brasiliano.com.br / mauro.ao@brasiliano.com.br
| site: www.brasiliano.com.br

"Fraudadores atacam todos os tipos de organização, o combate a eles é complexo e precisa de ações preventivas"

Gerenciando Riscos de Fraude através da sua Lógica

Antonio Celso Ribeiro Brasiliano

As fraudes não são privilégios somente desta época ou da sociedade atual. São tristes fatos que vêm se perpetuando pela história do homem e de suas civilizações.

Atualmente, as empresas estão percebendo cada vez mais que as fraudes também não são exclusivas de determinadas entidades ou ramos de negócios. Elas atacam qualquer tipo de organização, seja ocidental ou oriental; nacional ou multinacional; pública, mista ou privada; micro, pequena, média ou grande; sociedade anônima, limitada ou cooperativa; profissional ou familiar; rural ou urbana; com ou sem fins lucrativos; da área produtiva, comercial ou de serviços.

Vive-se hoje num mundo cultural, econômica e/ou mercadologicamente globalizado, onde as organizações enfrentam não mais uma concorrência local, regional ou setorial, mas a nível mundial.

A globalização econômica e o avanço acelerado das tecnologias vêm gerando, também, fraudes mais sofisticadas e condutas impróprias nas corporações. As consequências, para as empresas, tornam-se mais graves em termos de sanções aplicadas por agências regulatórias, danos de imagem, perdas financeiras e de confiança dos investidores, com desdobramentos

negativos que podem até afetar e influenciar cotações em bolsas.

Pesquisa realizada em 2006 pela 'Association of Certified Fraud Examiners', dos Estados Unidos, estima que as empresas norte-americanas perdem, a cada ano, 5% de seu faturamento por conta de fraudes. Levando-se em conta o PIB dos EUA em 2006, isso representaria uma sangria de US$652 bilhões/ano.

A fraude caracteriza-se pela ação intencional e com dolo praticado por agentes

internos ou externos, sejam colaboradores diretos da empresa, como seus prestadores de serviços alocados no ambiente empresarial, de forma não autorizada, com vistas a atentar contra os ativos empresariais suprimindo destes seus resultados.

Fraude não é apenas o furto comum, pela subtração direta de bens, mas toda forma de lesão ao direito de terceiros, tramada por artifícios executados por meio de métodos e práticas desonestas, ou seja, a fraude é todo ato intencional destinado a assegurar ganhos ilegais. É uma conduta imprópria, infringindo os princípios da ética e dos valores morais.

É preciso ficar atento sobre a questão da ética e dos valores morais, pois um dos grandes fatores que vem fazendo com que as fraudes cresçam no mundo corporativo é justamente a ausência dos mesmos. Há a necessidade de a empresa possuir um código de conduta e de ética definidos, estabelecendo a fronteira entre o ilegal e o ilícito. Não se pode esquecer que o maior problema do homem como ser humano é sua eterna luta entre a ética pessoal e a ética civil, a escolha entre o individual e o coletivo. A fronteira deve estar muito clara para todos os níveis da empresa.

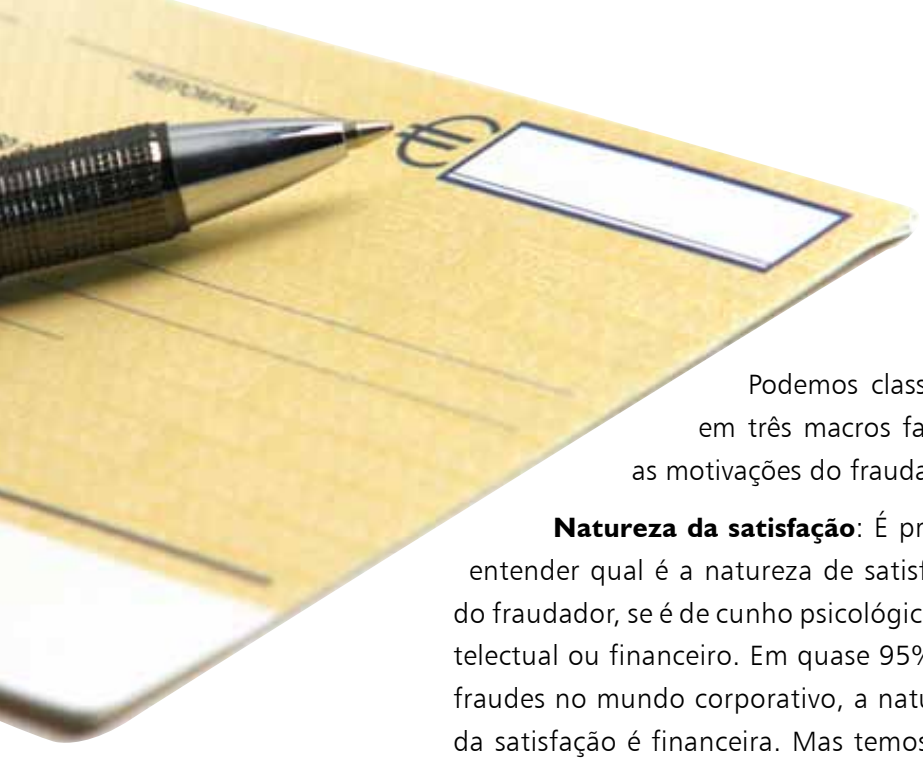
Diante do quadro de crescimento e progressão geométrica das fraudes, cada esforço desprendido eficazmente, cada economicidade realizada nos processos produtivos fará grande diferença. Ao contrário, cada erro, falha, desvio, perda e/ou desperdício será um fardo cada vez mais pesado e difícil de suportar.

As fraudes provocam, além das altas perdas financeiras, outras conseqüências por demais devastas. No âmbito do ambiente de trabalho, criam um clima de insegurança e desconfiança entre os funcionários e suas chefias. No âmbito da direção geral da empresa, provocam suspeitas e desconfianças sobre a capacidade de gestão de seus administradores. No âmbito externo, maculam a imagem da organização junto ao público consumidor.

Antes, no Brasil, as fraudes quase nunca eram percebidas devido à elevada inflação, que mascarava as perdas financeiras e também não levavam os administradores a observar com mais atenção o problema. As perdas por erros e irregularidades eram incorporadas aos custos da operação e repassadas ao consumidor. Eram poucas as empresas que possuíam em seus quadros auditores internos focados para a identificação preventiva de fraudes ou a auditoria denominada por nós como auditoria investigativa. Com a estabilização da moeda, advinda com o Plano Real, o problema tornou-se visível para a maioria das organizações.

LÓGICA DO FRAUDADOR

Para que se possa entender de forma clara como pensa o fraudador, é preciso estudar três fatores, visando identificar a lógica de agressão. São eles: motivações do fraudador; causas e oportunidades e a lógica e/ou a estratégia do fraudador.



Podemos classificar em três macros fatores as motivações do fraudador.

Natureza da satisfação: É preciso entender qual é a natureza de satisfação do fraudador, se é de cunho psicológico, intelectual ou financeiro. Em quase 95% das fraudes no mundo corporativo, a natureza da satisfação é financeira. Mas temos que procurar identificar as condições ambientais. Como exemplo se pode citar o caso de um funcionário que foi preterido na promoção por outro mais jovem e com menos tempo de empresa. Ele pode ficar magoado e a partir daí racionalizar que pode desviar recursos, já que a empresa não valorizou seu tempo de dedicação. Por esta razão, é necessário o perfeito entendimento da natureza da satisfação do fraudador.

Aposta do fraudador em ser descoberto: o fraudador, para cometer a fraude, tem que identificar as oportunidades, que podem variar desde a eficácia dos controles internos da empresa, indo para o perfil dos auditores e da equipe de investigação. Este fator é muito importante, pois é nele que o fraudador vai se basear para continuar na sua empreitada.

Expectativa de punição: neste fator, o fraudador avalia a política da empresa, seus pontos fracos em relação a condutas semelhantes, a legislação e a política de punição da empresa. O quanto a empresa está disposta em se expor para seu mercado, o quanto a divulgação de uma fraude pode impactar na imagem da instituição. Este é outro ponto importante, pois na verdade o fraudador pode até ser descoberto. Mas qual é a real chance de ser punido? Quanto tempo leva para que o inquérito saia da delegacia e vá para o Judiciário? A empresa possui provas contundentes ou somente suposições?

Com base no estudo destes três fatores, pode-se identificar a real motivação, ou seja, o quanto o fraudador está disposto a investir na continuidade do delito.

OPORTUNIDADES

O segundo fator estratégico é identificar as causas que potencializam a fraude no processo ou área que se está estudando. Para isso, deve-se pensar como um fraudador, imaginando como burlar os controles e sistemas de segurança existentes. Eles, de fato, podem bloquear as oportunidades? Temos o controle efetivo sobre o processo? O grande lance é identificar quais são os pontos frágeis, pois o fraudador conhece o processo. Não se pode esquecer que o fraudador é inimigo íntimo, é colega de trabalho, conhece todo o processo e terá que agir nos pontos considerados vulneráveis.

Sabendo o nível de motivação do fraudador, como os pontos considerados frágeis no processo, se tem plena condição de projetar qual será a lógica da agressão. A estratégia que o fraudador irá utilizar está embasada nestes dois pontos: motivação e fragilidade dos controles.

Entendendo estes três fatores, há condição de compreender a dinâmica da fraude, podendo-se implantar reais processos preventivos. Ressaltamos que, quando houver boa motivação e fragilidades de controles, a fraude tende a acontecer, independente das consequências e/ou punição. A cabeça do fraudador estará preparada para

suportar a pressão da punição, dependendo do ganho que ele terá.

Como exemplo, temos o caso de uma ex-funcionária que fraudou o INSS, que ficou presa em sistema especial em um quartel da Polícia Militar do Rio de Janeiro e quase nada foi recuperado. Outro exemplo é o caso do juiz Nicolau, de São Paulo, que está em regime de prisão domiciliar e também nada foi recuperado.

TIPIFICAÇÃO

Segundo a pesquisa da KMPG de 2004, os departamentos mais afetados são o financeiro (39%) e a área de compras (29%), enquanto as formas mais usuais de fraudar são por cheques ou documentos burlados (37%), roubo de ativos da empresa (33%), apresentação de falsas notas de despesas (30%) e notas fiscais frias (23%).

Esses percentuais cresceram em relação à pesquisa de 2002, quando a falsificação de cheques/documentos foi de 34%. As falsas notas de despesas representavam 24% e o item 'notas fiscais frias' gerou 16% das respostas. O roubo de ativos manteve-se em 33%. As propinas também tiveram um aumento no índice de resposta, passando de 10% para 14%.

A maior parte das perdas (83%) é inferior a R$1 milhão. Todavia, quase 50% das empresas não as recuperam. Mais da metade das empresas participantes da pesquisa descobriu a fraude por meio de seus controles internos (52%). A auditoria e a revisão interna também foram formas de constatar um grande número de atos fraudulentos (39%). Quase 30% receberam informações de seus próprios funcionários.

Após a descoberta de fraudes, a maioria das empresas (60%) demitiu os envolvidos e quase a metade delas (29%) apresentou queixa criminal contra os fraudadores. As investigações - tanto internas como externas - representam 33% das medidas adotadas.

Os pedidos de indenização permaneceram no mesmo patamar da pesquisa de 2002 (11%), enquanto a comunicação à seguradora decresceu de 5% para 2%.

CONHECER PARA AGIR

Só a metade dos fraudadores foi processada. Quantos foram realmente punidos? Faltaram provas? Faltou política de punição? Houve real interesse em punir os fraudadores? São perguntas que devemos procurar responder, pois caso contrário os processos preventivos de nada adiantarão por não se conseguir achar a verdadeira raiz do problema.

São de importância fundamental o levantamento e o estudo dos fatores motivacionais, pois a partir do momento em que os conhecemos com mais profundidade e se tem consciência da sua dinâmica, pode-se tomar reais ações preventivas. O conhecimento dos fatores e perfis do fraudador dá condições de, a partir dos indícios, traçar táticas para detectá-las e iniciar uma investigação com a brevidade que é necessária.

Um sistema detectivo de fraudes só será eficiente quando do entendimento desta dinâmica, que exige a integração do conhecimento do investigador e/ou auditor de inúmeras disciplinas. Esta complexidade será minimizada com a construção da lógica do fraudador, evidenciando a sua estratégia de agressão.

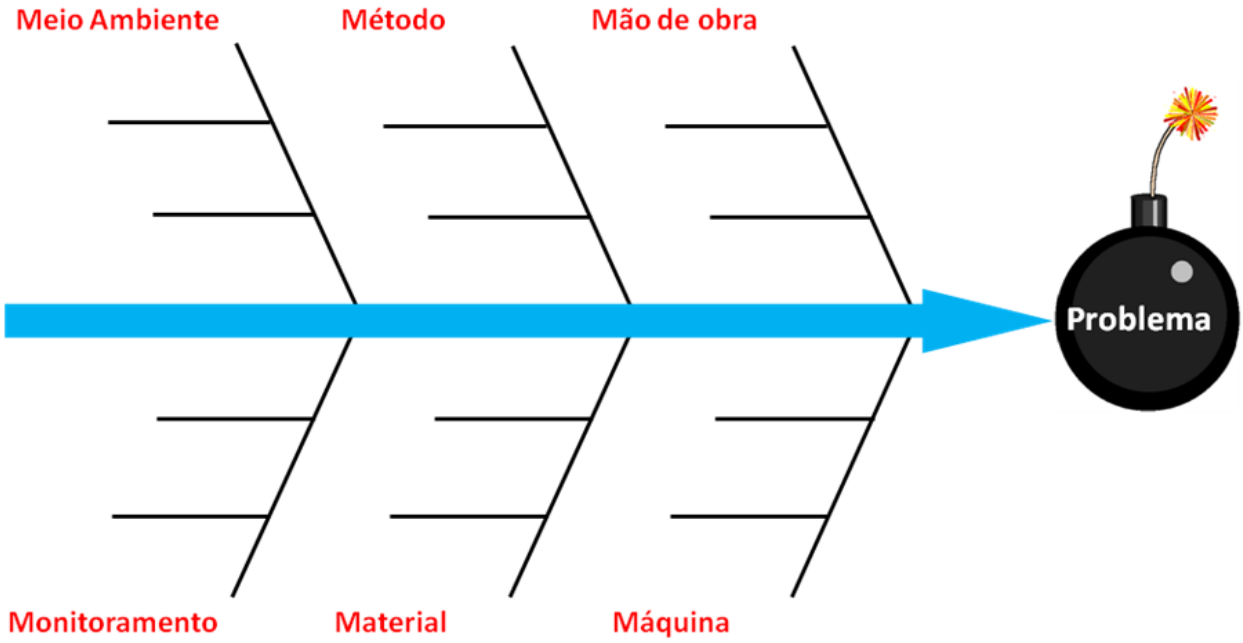
Antonio Celso Ribeiro Brasiliano
Publisher da Revista Gestão de Risco
e Diretor da Brasiliano & Associados
abrasiliano@brasiliano.com.br

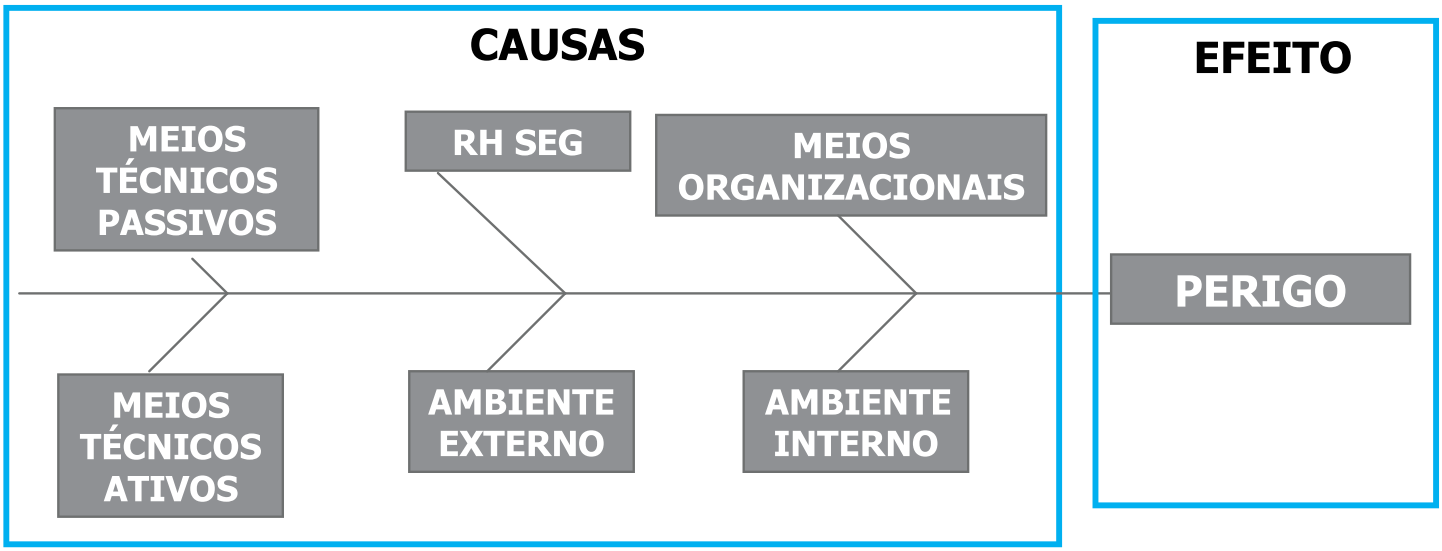
sumário

Aplicação do Diagrama de Causa e Efeito no Processo de Análise de Riscos

Gustavo Cirelli

Atualmente, a ferramenta conhecida como Diagrama de Causa e Efeito - Ishikawa - é uma adaptação feita para área de gestão de riscos, com o objetivo de identificar os fatores facilitadores, ou seja, as causas dos perigos estudados. Sua versão original foi criada durante uma reunião de engenheiros de uma fábrica do Japão. Seu criador, professor Karou Ishikawa, da Universidade de Tóquio, sintetizou as opiniões dos engenheiros enquanto eles discutiam problemas de qualidade. Portanto, em 1953, seu modelo original tinha como forma uma espinha de peixe dividida em seis macros fatores, sendo eles denominados de 6M: Mão de Obra, Método, Meio Ambiente, Máquina, Material e Monitoramento. O diagrama abaixo exemplifica:





Ele passou a ser implantado na gestão de qualidade e de outros processos empresariais. Para a área de gestão de riscos, as adaptações feitas buscaram facilitar a visão dos gestores, substituindo e dando definições aos seis macros fatores, inseridos no diagrama, nos meios organizacionais, nos recursos humanos de segurança, nos meios técnicos passivos, nos meios técnicos ativos, nos ambientes interno e externo.

OS FATORES SÃO:

Meios Organizacionais: é o levantamento feito se a empresa possui normas de rotina e de emergência, políticas de tratamento de riscos, gerenciamento de riscos, entre outras. A não formalização ou o não detalhamento pode ser um fator de influência para a concretização do perigo;

Recurso Humano da Segurança: é o levantamento do nível de qualificação, quantidade e posicionamento tático da equipe;

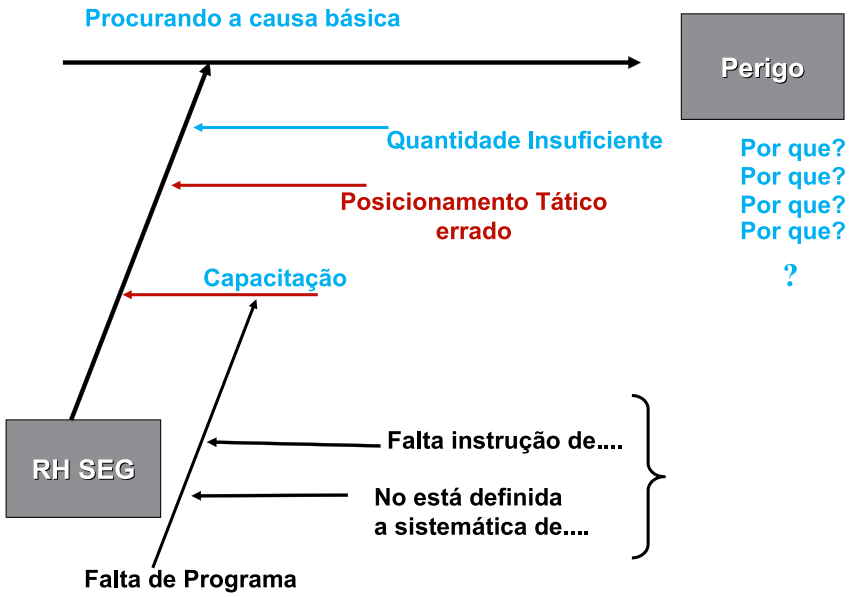
Meios Técnicos Passivos: é o levantamento da não existência de recursos físicos, tais como layout de portaria, salas, resistências de paredes e vidros, entre outros;

Meios Técnicos Ativos: é o levantamento da não existência de sistemas eletrônicos, desde CFTV, controle de acesso, sensoriamento, sistemas de rastreamento às centrais de segurança;

Ambiente Interno: é o levantamento do nível de relacionamento entre colaboradores e empresa. Inclui desde políticas de remuneração até políticas de recursos humanos;

Ambiente Externo: é o levantamento de cenários prospectivos, identificando fatores externos incontroláveis, mas que influenciam na concretização de perigos. Inclui o levantamento dos índices de criminalidade, estrutura do crime organizado, mercados paralelos, estrutura do judiciário, corrupção policial e ambiência no entrono, entre outros.

A técnica para detalhar os fatores é utilizar a pergunta 'por quê' até se esgotar o respectivo fator. O objetivo é identificar quais subfatores influenciam na concretização do perigo. O risco passa a ser, então, o somatório dos fatores. O Diagrama de Ishikawa é o risco, é a condição. Ele pode ser exemplificado pelo diagrama abaixo:



No processo de análise de riscos, os gestores devem utilizar o diagrama para mapear os subfatores (causas) de acordo com o perigo levantado, não se esquecendo de obter o entendimento do negócio da empresa e o contexto, além das características conjunturais em seu entorno. Desta forma, os gestores, com base nestas premissas e suas experiências, poderão identificar riscos coerentes ao negócio de sua empresa, independentemente do setor. Outro ponto importante para a correta aplicação da ferramenta é que a identificação dos riscos e os fatores de riscos devem ser discutidos em equipe, em uma reunião de 'brainstorming'. O diagrama ao lado mostra um exemplo:

Ao longo do tempo, o diagrama de causa e efeito (Ishikawa) sofreu outra adaptação direcionada a área de fraudes. Novamente, os macros fatores foram modificados para o gestor entender e mensurar as causas, deixando o diagrama com os seguintes macros fatores: controles alternativos, falhas prováveis, lógica do agressor, aposta do agressor, lógica da agressão e motivação do agressor.

OS FATORES SÃO:

Controles alternativos: existem controles alternativos para suprir as deficiências ou trabalhar em duplicidade?

Falhas prováveis: quais os controles existentes que possuem maior probabilidade de ser ludibriado ou não funcionar?

Lógica do agressor: como ele irá burlar os sistemas existentes?

Aposta do agressor: Pensando como fraudador, como que ele apostaria tendo em vista sua descoberta e qual a expectativa de punição?

Lógica da agressão: como os fraudadores poderiam agir, tendo em vista nosso 'status quo' de controle, serviços, cultura e perfil de recursos humanos?

Motivação do agressor - Natureza da Satisfação: que fatores motivam o fraudador a cometer o delito?

O segredo de uma boa investigação está em estabelecer a origem de cada risco, ou seja, identificar claramente cada fator de risco. Para isso, o gestor deve considerar as definições acima, lembrando sempre que as causas devem ser levantadas em reuniões de 'brainstorming', com as pessoas envolvidas na situação de risco definido, utilizando o Diagrama de Causa e Efeito ou 'espinha de peixe'.

Portanto, diante de dois exemplos em que a ferramenta Diagrama de Ishikawa pode ser utilizada, é possível mensurar a importância desta fase no processo de análise de riscos.

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

sumário

Formação de Auditor Líder em Gestão de Riscos

Álvaro Takei

O cenário atual demonstra que as empresas devem adotar um novo posicionamento, no sentido de possuir eficaz capacidade de resposta em casos de crises e riscos inerentes a sua atividade. A eficácia deve estar aliada à urgência, uma vez que a tecnologia propicia a difusão imediata de qualquer acontecimento, o que gera a necessidade de dar, rapidamente, satisfações a todos os que possuem interesses na organização, os chamados *stakeholders*.

Há, também, a intensificação da procura por medidas e métodos que possam minimizar ou mitigar os riscos potenciais de todos os processos em andamento na empresa, precavendo-se com o que venha a macular a imagem perante acionistas e o mercado como um todo. Isso passa a ser atividade importantíssima para as organizações que queiram garantir segurança, estabilidade e crescimento sustentado. Amplia muito a atividade de detectar possíveis falhas em registros e históricos contábeis, além de analisar seus impactos financeiros.

O novo posicionamento exige, ainda, que o conjunto de técnicas utilizado, não apenas auxilie na detecção e mensuração de possíveis problemas, como também ajude na indicação de soluções. Dentre as técnicas tem tido cada vez mais destaque as políticas de gestão de risco relacionadas a auditoria interna.

Neste contexto, a auditoria interna fica em evidência e adquire força, somente, se for além do zelo com relação à confiabilidade das informações prestadas, da análise do desempenho da gestão da empresa, do acompanhamento e controle do que foi traçado na estratégia, da avaliação de aspectos como governança corporativa e *compliances*. Desta forma, é preciso que colabore, ativamente, nos processos relacionados aos riscos corporativos, criando alertas para situações mais graves ou riscos negativos.

Estamos falando, portanto, que a postura da auditoria interna, como mera indicadora de problemas ou falhas, necessita modificar, acrescentando a prevenção, redução ou mitigação dos riscos, tendo em vista a competitividade empresarial, que exige eficiência e produtividade. Atender a estas expectativas passa a ser atribuição desta área estratégica de apoio. Caso estas necessidades não sejam atendidas, a auditoria interna poderá sofrer redução orçamentária ou mesmo extinção.

Fica claro, então, que ao falarmos que a auditoria interna deve evoluir, estamos dizendo que os profissionais que a compõe também devem evoluir, obtendo conhecimentos sobre gerenciamento de riscos. A categorização dos riscos em macro fatores é um primeiro conhecimento necessário. Isto permitirá a classificação dos riscos inerentes a cada macro fator, o que possibilita a analise, mapeamento e decisão sobre a priorização e destinação de recursos para monitoramento de riscos. Em seguida, é necessário verificar a probabilidade de ocorrência e possíveis impactos, tudo isto com intenso uso de ferramentas e métodos.

Resumindo, a gestão de riscos exige, no mínimo, os seguintes conhecimentos:

- Identificação de riscos potenciais;
- Mapeamento de riscos;
- Análise de riscos;
- Avaliar custos de prevenção x impactos financeiros;
- Elaboração de planos de prevenção;
- Administração de riscos ocorridos;
- Domínio de ferramentas e técnicas; etc.

Em outras palavras, queremos dizer que o auditor interno deve ser capaz de apoiar a desafiadora habilidade de monitorar, enfrentar e controlar o risco, e não, erroneamente, temê-lo. Dessa maneira, irá muito além de agir sobre fatos passados, contribuindo efetivamente para o desenvolvimento futuro das empresas.

Resta acrescentar que muitos dos riscos estão associados ao comportamento humano, motivo pelo qual outro desafio, que se afigura para o auditor, é o de compreender a natureza humana. Visa poder levar em conta as suas atividades, bem como usar essa compreensão no relacionamento com todos os integrantes da organização, fazendo com que o conhecimento sobre pessoas, aliado ao conhecimento técnico da atividade, faça dele um Auditor Líder.

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

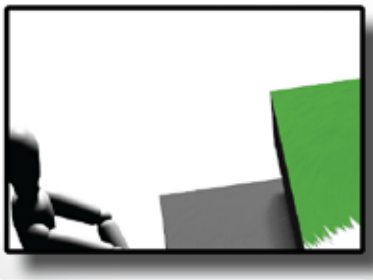
sumário

FAÇA A DIFERENÇA !!!!

Porque os cursos da Brasiliano?

DISSEMINAÇÃO é a palavra chave da área de treinamento, pois acreditamos que o conhecimento é para ser compartilhado com qualidade, credibilidade e ousadia.

Por este motivo, é que grandes profissionais de sucesso atingiram seus objetivos



Especialização e Extenção Universitária

Cursos Digitais

PÓS-GRADUAÇÃO MBA

Cursos Presenciais

convênio:
Fapi e Fesp

FAPI FACULDADE DE ADMINISTRAÇÃO SÃO PAULO

FESP FACULDADE DE ENGENHARIA SÃO PAULO

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

b&a
BRASILIANO&ASSOCIADOS

Gestão de Riscos Corporativos e Ferramenta de TI Audixpress

Fernando de Bonneval de Carvalho

No contexto mundial de negócios, empresas, independentemente de seu porte, acabam desaparecendo do mercado por falta de conhecimento. Elas não conseguem pensar do 'lado de fora da caixa' e acabam deixando de levar em conta critérios essenciais para sua sobrevivência. Um dos principais ativos de uma organização é a informação, pois é o conjunto que servirá como base para a empresa montar sua estratégia de negócio. As organizações devem, então, buscar continuamente dados para auxiliar nas decisões e quais estratégias serão adotadas naquele determinado contexto em que estão inseridas.

Apenas reagir não é mais suficiente para garantir a sobrevivência da empresa no mercado. A organização deve ter uma visão prospectiva, que antecipe os fatos, através da otimização das informações obtidas. Devido ao alto nível de concorrência no mercado atual, um pequeno detalhe pode significar diferenciação competitiva para a organização.

Com o desenvolvimento da Tecnologia da Informação (TI), as organizações têm ferramentas que auxiliam na sua estratégia de negócio, otimizando os processos e diminuindo o tempo de execução de determinadas tarefas graças a automação. Segundo o Mestre em Ciência da Computação Eduardo Mayer Fagundes (Como ingressar nos negócios digitais), "é impossível imaginar uma empresa sem uma forte área de Sistemas de Informações para manipular os dados operacionais e prover informações gerenciais aos executivos para tomadas de decisões". Ou seja, a sobrevivência da empresa depende da utilização da Tecnologia da Informação como vantagem competitiva.

Porém, uma má escolha ou uma má utilização da ferramenta de TI fará com que a organização desapareça do mercado, pois ela não con-

seguirá aliar estratégia de negócio com a ferramenta de TI. Os gestores, consultores e analistas devem, então, dominar, adequar a ferramenta de TI às necessidades de sua organização.

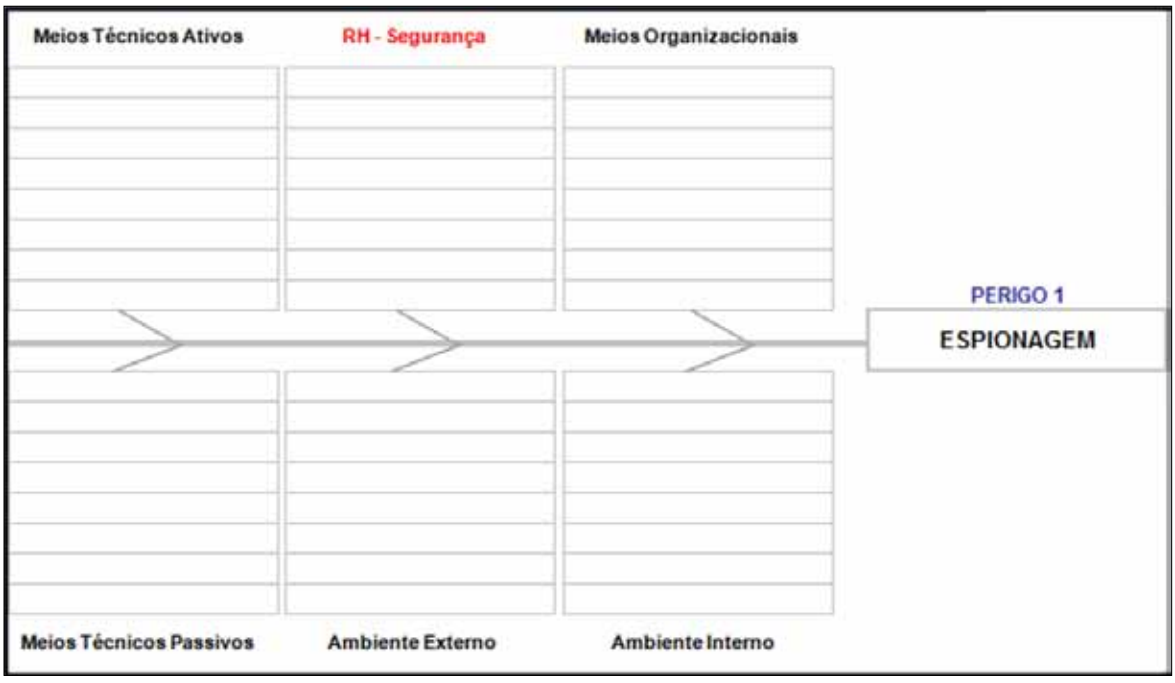
As organizações acabam errando na hora de escolher uma ferramenta TI para ser implantada, pois elas não levam em conta:

- A ferramenta não pode ser totalmente automatizada, deve haver percepção do gestor;
- A ferramenta de TI não pode ter uma metodologia própria;
- A ferramenta de TI deve ser flexível e adaptada para o negócio da organização;
- A ferramenta de TI não pode ter critérios amarrados, pois cada negócio possui características distintas.

Na área de gestão de riscos, as organizações selecionam um modelo de ferramentas de TI com o mesmo objetivo: automação, otimização dos recursos e antecipação por meio de simulações. Isso significa que na Gestão de Riscos, os processos precisam ser aprimorados para que a organização consiga aumentar eficiência, melhorar a qualidade, reduzir seus custos internos para ganhar velocidade e desempenho na entrega de seus produtos e serviços.

Portanto, o objetivo da ferramenta de TI na Gestão de Riscos é auxiliar a organizar e gerenciar riscos de uma maneira simples, eficiente, produtiva, customizada e flexível. O sistema da ferramenta permite que o gestor tome decisões em fatos reais, correlacionando riscos, controles e melhore práticas do mercado, graças a possibilidade em criar simulações. Porém, para ser eficiente, a ferramenta de TI deve respeitar certos critérios.

As organizações devem evitar, a qualquer custo, que a ferramenta seja amarrada ao processo ou que ela seja totalmente automatizada, pois a consciência do utilizador é essencial na Gestão de Riscos Corporativos. A organização não pode 'comprar um pacote fechado'. Antes de implantar uma ferramenta de TI para auxiliar na Gestão de Riscos, a organização deve verificar que ela esteja em harmonia com os métodos desenvolvidos de processos gerenciais e organizacionais, ou seja, a ferramenta de TI deve ser convergente ao 'Core Business' da organização.



Na Gestão de Riscos Corporativos, uma ferramenta de TI eficiente deve comportar obrigatoriamente:

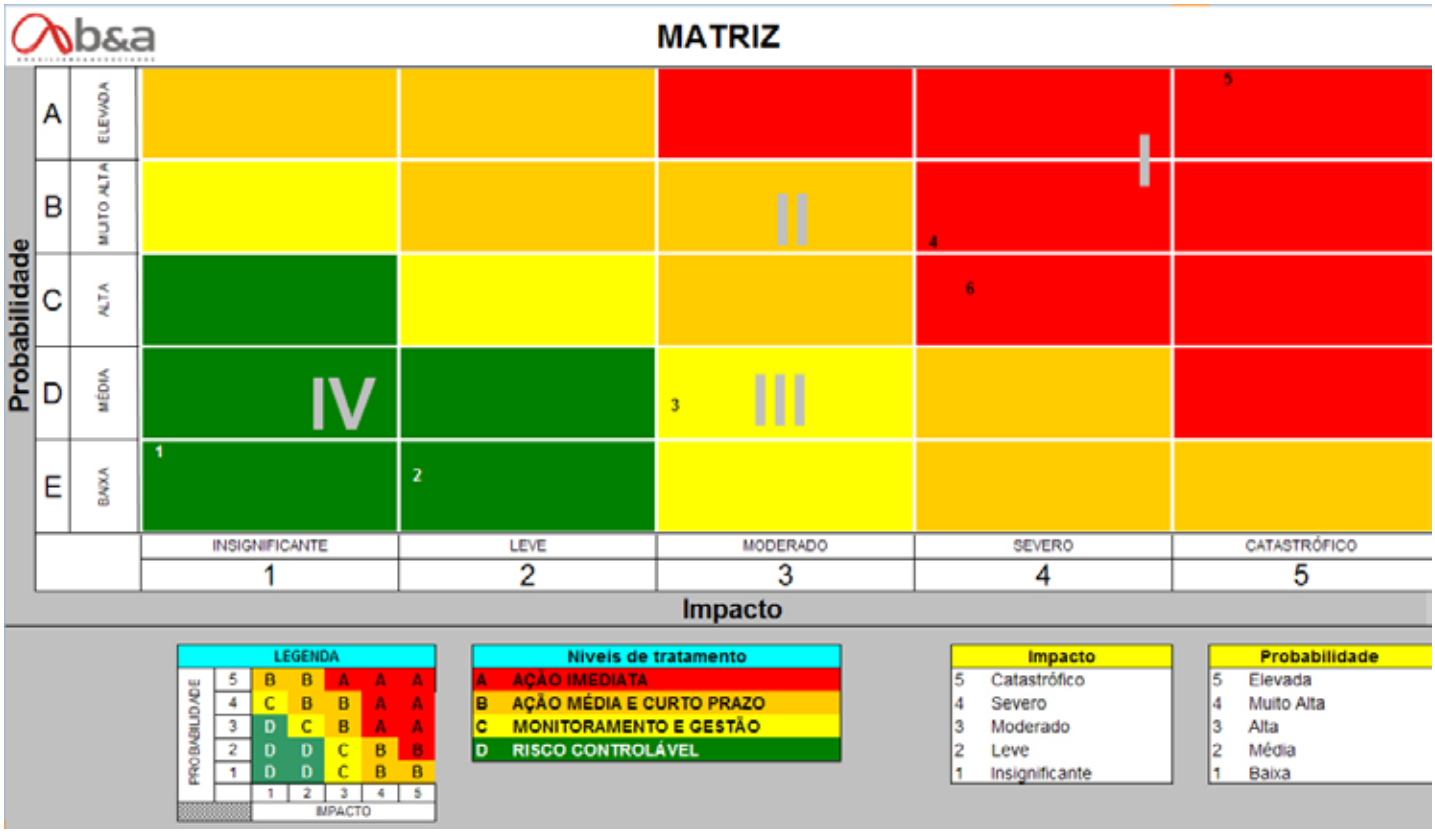
- Banco de dados atualizável: regulamentações; melhores práticas e metodologias existentes; conceituação de eventos por área de negócios;
- Metodologia customizada: informação auditoria; Gestão de Riscos do Negócio; Gestão de Riscos de Segurança; Fraudes; Plano CE Continuidade de Negócios;
- Critérios de criticidade;
- Informações.

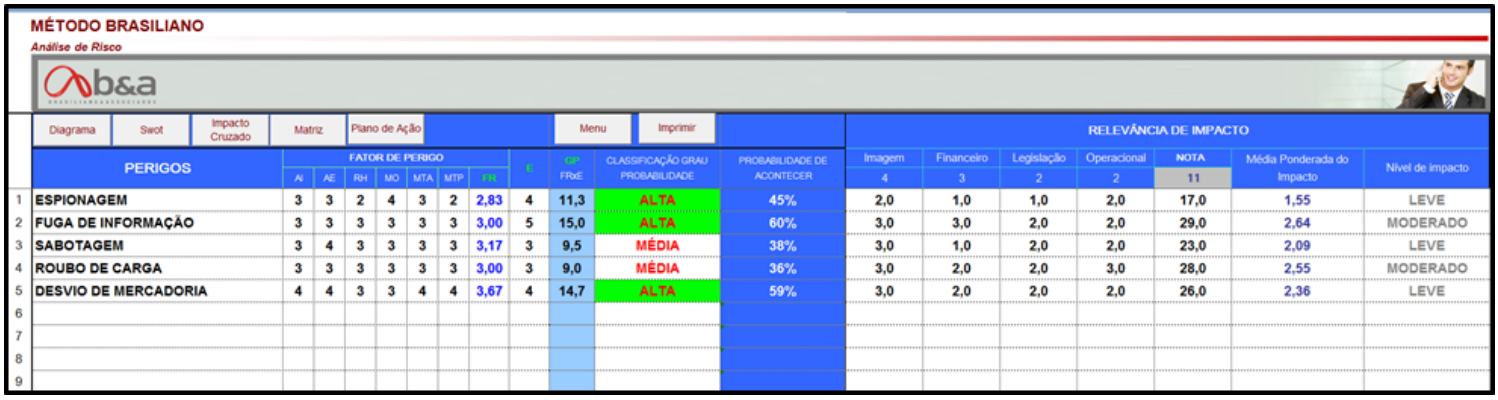
Entretanto, uma ferramenta de TI na Gestão de Riscos Corporativos eficiente deve ser, imperativamente, de fácil utilização para o usuário, pois o software deve auxiliar e facilitar o trabalho. No mercado, existem diversas ferramentas de TI para auxiliar na Gestão de Riscos Corporativos de uma organização, porém, o desafio da organização é saber escolher a melhor ferramenta que possa suprir suas necessidades para sobreviver no mercado.

Um exemplo de serviço de implantação de ferramentas estratégicas é o desenvolvimento da gestão de riscos corporativos, chamada Audixpress.

A Brasiliano, em parceria com a Murah Teachnologies, desenvolveu a ferramenta de TI Audixpress, que importou os processos da metodologia Brasiliano e Associados. A missão desta ferramenta de TI é agregar valor e facilitar a operação e controle através de ferramenta de TI, de maneira personalizada e otimizada, economicamente adequada e focada no 'Core Business' da organização.

A Audixpress (www.brasiliano.com.br) é uma ferramenta diferenciada que oferece de forma única e integrada a gestão de auditoria, riscos, controles internos, compliance e continuidade de negócios, aderente às normas, regulamentações, leis e frameworks como BACEN 3380, COSO,





MÉTODO BRASILIANO

Análise de Risco

b&a

Diagrama | Swot | Impacto Cruzado | Matriz | Plano de Ação | Menu | Imprimir

	PERIGOS	FATOR DE PERIGO AI	AE	RH	MO	MTA	MTP	FR	E	GP FRxE	CLASSIFICAÇÃO GRAU PROBABILIDADE	PROBABILIDADE DE ACONTECER	RELEVÂNCIA DE IMPACTO Imagem 4	Financeiro 3	Legislação 2	Operacional 2	NOTA 11	Média Ponderada do Impacto	Nível de impacto
1	ESPIONAGEM	3	3	2	4	3	2	2,83	4	11,3	ALTA	45%	2,0	1,0	1,0	2,0	17,0	1,55	LEVE
2	FUGA DE INFORMAÇÃO	3	3	3	3	3	3	3,00	5	15,0	ALTA	60%	3,0	3,0	2,0	2,0	29,0	2,64	MODERADO
3	SABOTAGEM	3	4	3	3	3	3	3,17	3	9,5	MÉDIA	38%	3,0	1,0	2,0	2,0	23,0	2,09	LEVE
4	ROUBO DE CARGA	3	3	3	3	3	3	3,00	3	9,0	MÉDIA	36%	3,0	2,0	2,0	3,0	28,0	2,55	MODERADO
5	DESVIO DE MERCADORIA	4	4	3	3	4	4	3,67	4	14,7	ALTA	59%	3,0	2,0	2,0	2,0	26,0	2,36	LEVE
6																			
7																			
8																			
9																			

COBIT, ISO 27001, ISO 27002, NBR 15999, ITIL, SOX e outros. É uma tecnologia multi-forma, baseada em padrões aberto e Web, desenvolvida sob tecnologia Java.

A solução desta ferramenta se divide em três camadas: a camada de negócios contempla as funcionalidades executadas sob container e servidor de aplicação; a camada da visualização é executada através de um browser, e a camada de persistência é representada por três bases, que compreendem o banco de dados relacional, base de dados textual e sistemas de arquivos.

A Audixpress possui uma estrutura extremamente flexível e dinâmica, que se ajusta a qualquer modelo de negócio e auditoria, aplicando-a em processos de auditoria em qualidade, conformidade, contábil, fiscal, financeiro, ambiental, fiscalização, inspeção, investigação, recursos humanos, controles internos, segurança da informação, TI, hospitalar e outros.

Os principais benefícios na utilização da Audixpress são:

- Dados em banco de dados;
- Acompanhamento automatizado do trabalho de auditoria por meio de notificações, relatórios e gráficos;
- Geração automática de relatórios;
- Dados consolidados em segundos;
- Segurança das informações com criptografia;
- Alta performance e foco produtivo na atividade chave;
- Acesso as informações controlado por perfis de usuários;
- Acesso rápido, simples e dados históricos.

A ferramenta Audixpress possui as seguintes aplicações:

- **Audixpress Audit:** definição dos ciclos de auditoria;
- **Audixpress:** bases de conhecimento e melhores práticas; Plano de Continuidade de Negócios: definição do PCN; Análise de Impacto no Negócio BIA; definição de responsabilidades; planejamento de recursos para continuidade; mapeamento dos incidentes e procedimentos operacionais; aderente a norma ABNT NBR 15999;
- **Compliance:** alinhamento da organização às normas, leis e regulamentos; melhores práticas de mercado; criação e importação das normas internas da organização para a base do sistema;

elaboração e aplicação de questionários de conscientização;

- **Controls:** definição das políticas e procedimentos que contribuem para assegurar as respostas aos riscos; classificações dos controles (preventivo ou detectivo e execução);
- **Core:** fácil criação de estruturas organizacionais; macro processos e sub processos, processos e atividades facilmente configuráveis; perfis de acessos flexíveis e configuráveis; logs de acesso ao sistema;
- **Dashboard:** visão executiva de indicadores por meio de um painel de controle; painel customizável; painéis em formato gráfico, de tabela, diagrama, etc;
- **KPI:** definição de indicadores chaves de performance para cada processo organizacional; avaliação dos indicadores ao longo do tempo; criação de Scorecard; visão dos indicadores pela estrutura organizacional e processos;
- **Report:** variedade de consultas em tempo real; padronização de documentos e relatórios;
- **Principais recursos:** elaboração flexível de modelos e documentos, geração de relatórios dinâmicos;
- **Risk:** módulo de gestão de risco que possibilita sua gestão integrada com os riscos da empresa. Acompanhamento, controle e testes de controle.

Portanto, as organizações, na hora de implantar uma ferramenta de TI, ligada à Gestão de Riscos Corporativos, devem verificar se a ferramenta tem a capacidade de se adequar as suas necessidades e estratégias. Para a organização, a ferramenta de TI ligada à Gestão de Riscos deve ser customizada de acordo com o contexto em que a organização está inserida.

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

"A ferramenta Audixpress possui:

- Audixpress Audit

- Audixpress

- Compliance

- Controls Core

- Dashboard

- KPI

- Report

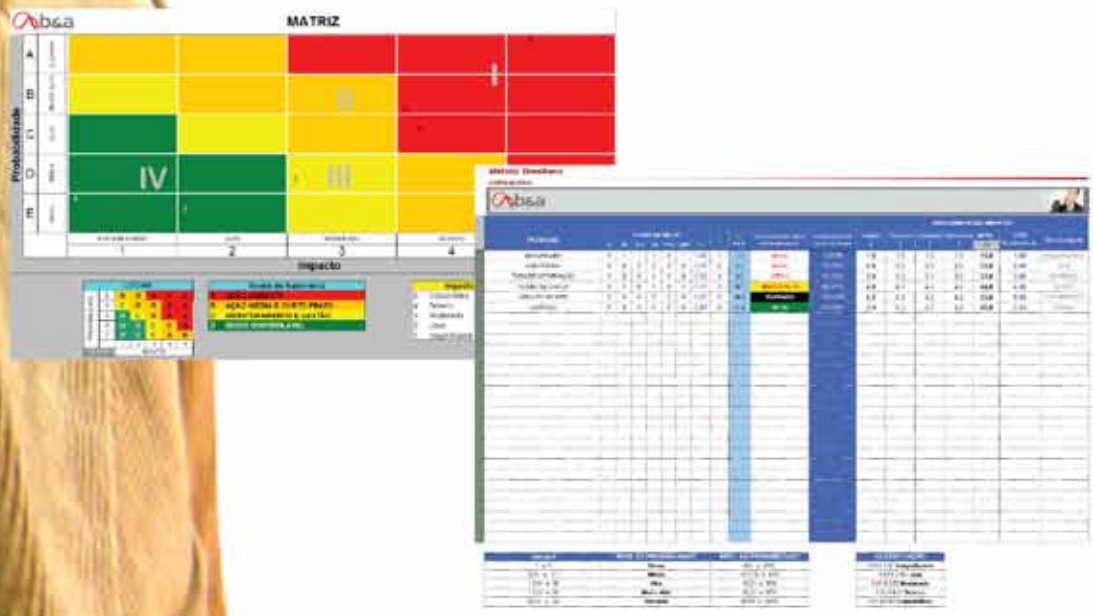
- Principais recursos

- Risk "

sumário

FERRAMENTA de TI sua solução SOB MEDIDA

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



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

murah audiXpress

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

b&a BRASILIANO&ASSOCIADOS

CFTV – Entendendo seu Funcionamento

Ricardo Yagi

Este artigo tem como objetivo dar uma visão geral sobre o CFTV: conceito, evolução das tecnologias de hardware, comunicação, software e padrões utilizados atualmente.

CFTV COMPOSTO POR CÂMERAS ANALÓGICAS E GRAVADOR ANALÓGICO (TIME LAPSE):

A primeira geração de CFTV, baseada em hardware, nasceu devido a necessidades de monitoramento e segurança; sua operação baseou-se em câmeras passivas ou "burras" e armazenamento "burro" (mecânico e sem poder de processamento).

Pontos Fortes:

1) As câmeras são instaladas com proteção contra intempéries, vandalismo e em locais de difícil acesso para eliminá-lo;
2) Inibe ações predatórias e criminosas na área do contexto visual;
3) Permite a gravação de imagens e áudio sem a necessidade de operadores;

4) Permite a ação imediata de segurança, com a atuação dos operadores que monitoram o ambiente.

Limitações:

1) Os operadores não permanecem vigiando todo o tempo, ocasionando perda de uma ação imediata para ocorrências importantes;
2) Qualidade de gravação baixa da imagem;
3) Perda de detalhes da ocorrência, pois por questões de economia, os time lapses (gravadores VCR de fita VHS) chegam a gravar de 12 fps (frames ou imagens por segundo) a até 960 horas (40 dias) e gravação de uma imagem a cada 12s.
4) Devido à reutilização constante, as fitas VHS se degradam, causando perda da qualidade das imagens;
5) Se acessível, os criminosos podem roubar ou inutilizar a fita;
6) Estrutura de cabos de difícil instalação e manutenção, devido a sua espessura e comprimento (de cada câmera parte um cabo para o switcher ou mutiplexador que pode estar a centenas de metros);
7) A localização de uma ocorrência é feita visualmente, procurando por toda a fita, o que demanda um tempo muito grande;
8) Necessidade de troca manual de fitas;
9) Acesso mecânico (fita VHS) às informações (imagens).

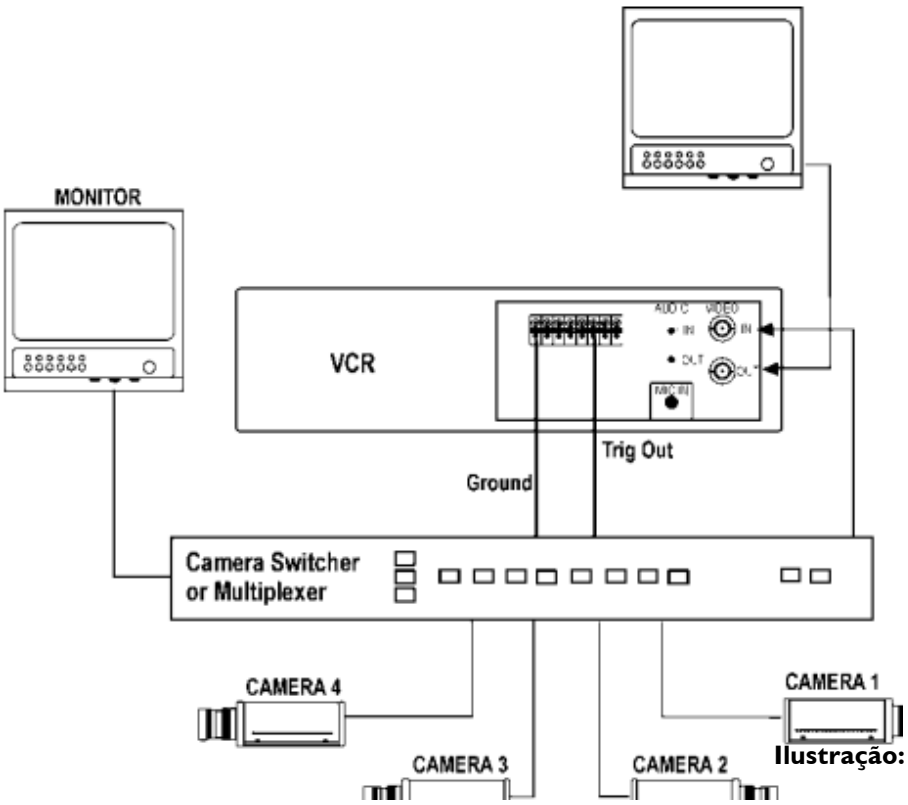


Ilustração: Sistema CFTV Analógico

CFTV COMPOSTO DE CÂMERAS ANALÓGICAS E DVR (GRAVADOR DIGITAL):

A segunda geração de CFTV, baseada em hardware, introduziu o DVR, que, além das funções básicas do "time lapse", trouxe uma grande gama de facilidade ao CFTV, consequentemente proporcionando maior versatilidade e maior eficácia ao sistema de segurança. Esta configuração representa 80% a 90% do parque instalado de CFTV no mundo.

O DVR "inteligente" substitui a gravação analógica pela gravação digital e adiciona recursos computacionais digitais para a estação de monitoramento e armazenamento.

Figurativamente, podemos substituir os dispositivos multiplexer e o VCR na ilustração ao lado, por um DVR tradicional.

Ilustração: Sistema CFTV Analógico

Pontos Fortes:

1) Seleção de imagens e modos de gravação digitais pré-programados;
2) O recurso "Motion Detection" ou detecção de movimento, permite que apenas haja gravação quando houver movimento, economizando espaço de gravação;
3) Maior qualidade da imagem gravada;
4) A localização de uma ocorrência é feita diretamente, baseada em eventos, datas e horários;
5) O acesso às informações/imagens é feito através de senhas;
6) A gravação e regravação são feitas ocupando um espaço previamente delimitado, sem perda de qualidade e sem parada do sistema;
7) Pode utilizar-se de compactação de imagens (Wavelet, JPEG, MPEG-4 ou H.264);
8) Capacidade de pré-programar o PTZ (Pan Tilt Zoom), que é a movimentação da câmera na horizontal, vertical e aproximação;
9) Back-up das imagens para DVDs;
10) Consultas real time remotas via Web.

Limitações:

1) Um segundo de gravação de imagens de boa qualidade ocupa até 5 MB, exigindo meios de compactação e armazenamento dimensionados e dedicados. Imaginem gravar as imagens de centenas de câmeras simultâneas;
2) A dificuldade da instalação e manutenção do cabeamento permanecem, existindo casos frequentes de impossibilidade de instalação ou expansão do número de câmeras desejáveis, devido a limitação de espaço e infra-estrutura (eletrodutos, calhas e conduítes) para a passagem dos cabos.

CFTV COMPOSTO POR CÂMERAS IP E NVR (NETWORK VÍDEO RECORDER):

A terceira geração, caracterizada ainda por inovações de hardware, foi a introdução de câmeras IP pela Axis, em 1996. A partir de então, as câmeras puderam ser consideradas 'inteligentes', pois tinham uma identidade digital IP, tinham capacidade própria de processamento e poderiam "conversar" diretamente com qualquer ponto da rede. Por consequência, temos então as 'duas pontas inteligentes'.

Em um sistema de redes IP, basta conectar as câmeras IP e o NVR ao barramento da rede para visualizarmos um sistema CFTV totalmente digital. Um ponto fundamental para esta implantação é a análise criteriosa da banda necessária e disponível para o tráfego na rede.

Pontos Fortes:

1) De um modo geral, tem a capacidade de analisar e processar imagens e sinais, independente do NVR e diretamente com outros sistemas da rede;
2) Trata a detecção de movimentos e outras funções internamente;
3) Recebe sinais diretamente de alarmes e sensores e interage com sistemas diversos, como controle de incêndio, controle de acesso ou outros;
4) Pode enviar imagens com um formato de menor resolução para fins de monitoramento e simultaneamente em outro formato de maior resolução para gravação pelo NVR;
5) Sua imagem pode ser acessada diretamente por qualquer dispositivo da rede;
6) A câmera IP se liga diretamente ao ponto de rede mais próximo (limite de 100m) através de cabo de rede normal, bem menos volumoso que no caso das câmeras analógicas, economizando material e tempo de instalação;
7) Pode ter a opção PoE (Power over Ethernet), que também facilita a instalação em termos de fornecimento de energia para o funcionamento da câmera;
8) Existem câmeras IP que tem funções especializadas (4ª geração), como por exemplo, 'contar pessoas' que passam a sua frente;
8) As câmeras IP wireless proporcionam a instalação mais fácil, pois necessita apenas de sua configuração lógica na rede e a fonte de energia para seu funcionamento.

Limitações:

1) O tráfego de imagens ou streaming de vídeo ocupa uma grande banda e deve ser feito um estudo de uma rede própria ou da rede a ser compartilhada, câmeras e codecs (formatos de vídeo) compatíveis para a instalação e operação eficiente, sem interferir na operação da empresa;
2) O preço de câmeras IP ainda é muito mais alto quando comparado a analógicas;
3) Muitas soluções de software NVR, que controlam a rede IP de câmeras, têm um número limitado de câmeras e modelos homologados;
4) Câmeras mais atuais chamadas Megapixel fornecem imagens de alta resolução e, portanto, maior banda para transmissão e armazenamento.

OUTRAS TECNOLOGIAS PARA CFTV:

A 4ª geração, baseada em software, utiliza de processamento de imagens (instalado na câmera ou na rede), denominadas "vídeo analytics", para tratar situações como: detecção de aglomeração, objeto esquecido ou deixado no meio de um saguão ou recepção, detecção de rota proibida para

veículos ou pessoas, reconhecimento de face, contagem de pessoas, reconhecimento de comportamento e outros.

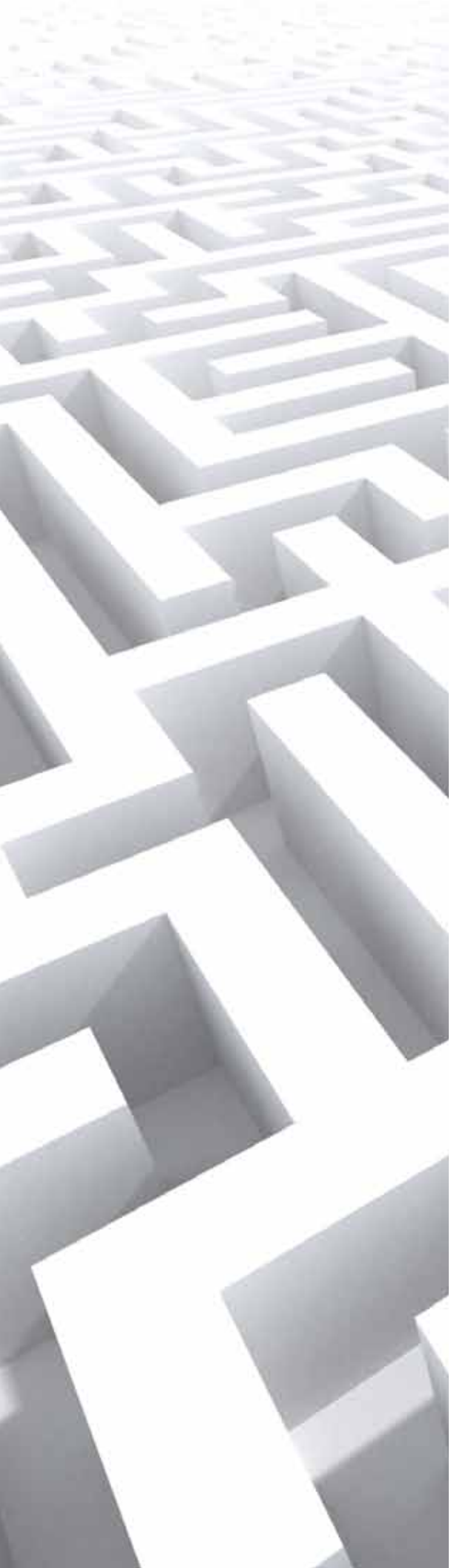
Outra utilização diferenciada é o CFTV com reconhecimento de placas voltada a segurança metropolitana instalada em Itatiba, que por meio de câmeras instaladas via fibra ótica em pontos estratégicos e software de redes neurais, trabalha em conjunto com a polícia para desvendar casos de roubo de lojas, carros, sequestros e tráfego de drogas, entre outros, diminuindo significativamente os índices de criminalidade.

Conclusão:

Esta foi apenas uma introdução técnica e básica. Para a elaboração de projetos, instalação, supervisão e manutenção de CFTV, são necessários estudos aprofundados. É preciso conhecer a grande diversidade de câmeras analógicas e digitais, codecs, dispositivos de comunicação e estudar as diversas composições de funcionalidades e compatibilidades entre os dispositivos disponíveis no mercado. Em seguida, a vivência com sistemas de CFTV e segurança é imprescindível para o domínio desta matéria.

Ricardo Yagi
Consultor da Brasiliano & Associados
yagi@brasiliano.com.br

sumário



Desinformação

Joffre Coelho Júnior

A Contra-Inteligência é o ramo da Atividade de Inteligência responsável em salvaguardar o Sistema da Empresa contra as ações dos seus concorrentes. É uma atividade permanentemente exercida e executada com o objetivo de proteger conhecimentos vitais para a empresa, seu pessoal e instalações contra as atividades desenvolvidas pelo Serviço de Inteligência da concorrência.

A desinformação é uma medida de caráter ofensivo, onde a empresa, por meio do seu departamento de Contra-Inteligência, irá iludir a concorrência sobre suas atividades e, principalmente, sobre o lançamento de seus produtos e/ou serviços. Para atender o que está descrito no conceito acima, a Contra-Inteligência adota dois segmentos: Segurança Orgânica e Segurança Ativa.

A Segurança Orgânica é o conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações do serviço de Inteligência da concorrência. Para isso, conta com os seguintes grupos de atividades:

- Segurança de Pessoal;
- Segurança da Documentação;
- Segurança das Comunicações;
- Segurança da Informática;
- Segurança de Áreas e Instalações.

A Segurança Ativa é a atividade desenvolvida pelo Serviço de Inteligência da empresa, com o objetivo exclusivamente ofensivo, visando detectar, identificar, avaliar e neutralizar as ações criadas pelo mesmo departamento da concorrência. Essa atividade é executada pelas seguintes ações:

- Contra-Espionagem;
- Contrapropaganda;
- Desinformação.

Nesse sentido, a Desinformação é a atividade que traduz em ganho significativo para a empresa, tornando-a mais competitiva atualmente, quando o risco se faz presente em todas as atividades, sejam elas de produto ou serviço.

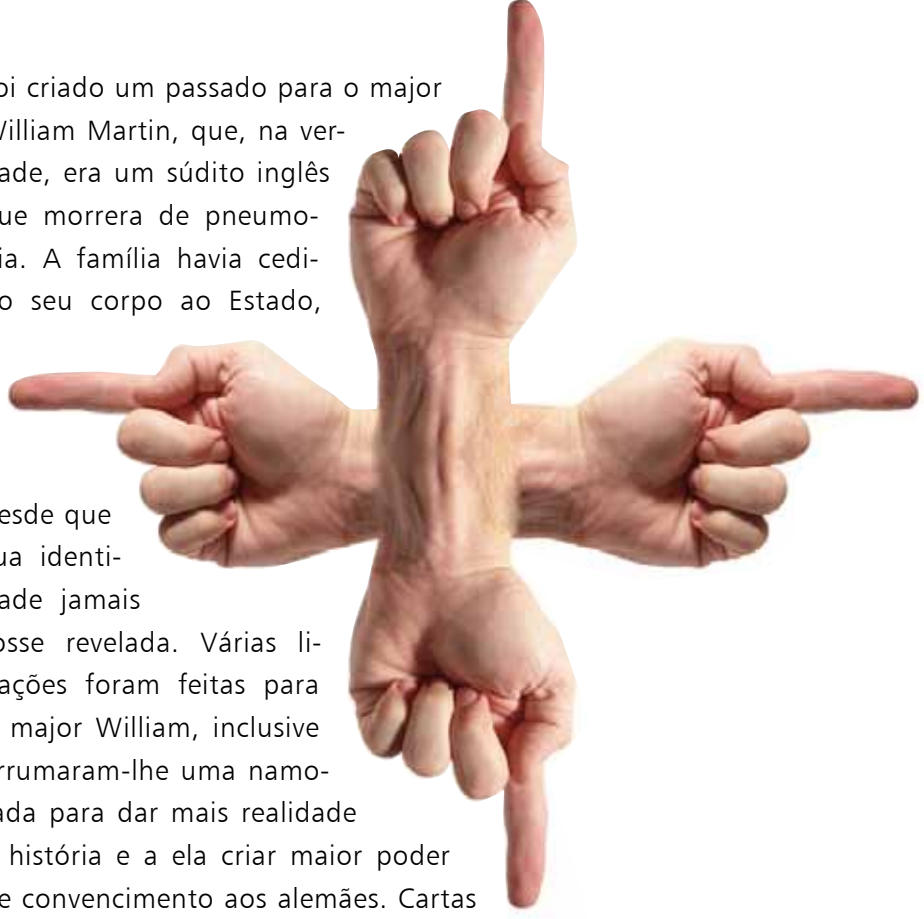
Um exemplo disso pode ser obtido na década de 40. Durante a

Segunda Grande Guerra, uma Operação do Serviço de Inteligência Britânico confundiu a Inteligência Alemã, obtendo êxito na invasão da Europa. Ela ficou conhecida como a mais bem sucedida Operação de Desinformação da Segunda Guerra Mundial. Daí surge a Operação *"Mincemeat – Recheio"*.

Após o sucesso da invasão da África do Norte, os estrategistas aliados queriam definir o próximo passo: avançar da África para a Europa pela Sicília, pelo Estreito de Messina. É claro que os alemães esperavam por isso e concentrariam suas forças na região. Como convencê-los do contrário, induzindo-os a dispersar suas tropas para outros pontos do continente europeu? A partir daí, um membro do 'Intelligence Service' britânico pensou na tal Operação de Desinformação.

Como os alemães sabiam que oficiais ingleses sobrevoavam a costa espanhola rumo à África do Norte, por que não lançar ao mar um cadáver com documentos falsos, como se fosse vítima fatal de um acidente aéreo, exatamente nas imediações do litoral espanhol?

A Operação foi planejada nos mínimos detalhes desde a escolha do cadáver, que deveria ter a *causa mórtis* as características de um afogamento para confundir os alemães - pois fatalmente isso seria verificado pelo Serviço de Inteligência Alemão - bem como todo o resto da *Estória de Cobertura*.



Foi criado um passado para o major William Martin, que, na verdade, era um súdito inglês que morrera de pneumonia. A família havia cedido seu corpo ao Estado, desde que sua identidade jamais fosse revelada. Várias ligações foram feitas para o major William, inclusive arrumaram-lhe uma namorada para dar mais realidade à história e a ela criar maior poder de convencimento aos alemães. Cartas e documentos foram dobrados e desdobrados várias vezes para parecer que tinham sido lidos diversas vezes.

O major Martin portava chapas de identificação, um relógio de pulso, cigarros, bilhetes antigos de ônibus e chaves. Em sua última noite na Inglaterra, teria levado a noiva ao teatro e tinha no bolso a metade de dois ingressos para uma peça no dia 22 de abril de 1942.

Em suma, o plano baseava-se nos seguintes pontos:

Martin levaria numa pasta uma carta do general Sir Archibald Nye, subchefe do Estado-Maior Imperial, ao general Alexander, comandante do Grupo de Exércitos da África, com uma explicação, 'entre amigos', dos motivos pelos quais Alexander não estava recebendo do chefe do Estado-Maior tudo o que queria. Por inferência, chegava-se a conclusão que se planejava atacar o Mediterrâneo Ocidental. Os possíveis pontos seriam: um na Grécia e outro não muito bem identificado, que não era a Sicília.

O major levava, ainda, um comunicado do Lorde Louis Mountbatten ao almirante de Esquadra, Sir Andrew Cunninghan, comandante e chefe no Mediterrâneo, explicando sua missão e concluindo: "Creio que Martin é o homem que lhe serve. Queira mandá-lo de volta logo que termine o assalto. E não se esqueça de dar-lhe mais sardinhas. Elas estão aqui racionadas".

A palavra 'sardinhas' servia apenas para indicar aos alemães a Sardenha como objetivo do ataque. Estava assim em grosso modo preparada, a Operação Recheio. O cadáver de Martin seria transportado pelo submarino Seraph, sob o comando do tenente Jewell, e lançado ao mar próximo a Huelva. O próprio Churchill deu sua aprovação e ordenou para que o general americano Eisenhower, no comando da invasão da Sicília, fosse informado.

A operação foi desencadeada e na manhã do dia 30 de abril de 1943, quando um pescador espanhol avistou o corpo perto da praia e avisou as autoridades. Após autópsia, constatou-se asfixia por imersão no mar.

Como os britânicos imaginavam, os documentos caíram nas mãos de um conhecido espião nazista operando na Espanha, que depois de fotografá-los enviou as fotos para a Alemanha.

Nesse ínterim, um agente alemão estava na Inglaterra verificando o passado de Martin, investigando os dados relativos a sua vida. Tudo que procurou, achou. Convenceu-se de que tudo era verdadeiro, e informou seus superiores na Alemanha, sem saber que a Contra-Inteligência havia seguido seus passos.

Como resultado, o alto comando alemão transferiu uma Divisão Blindada da França para o Peloponeso (região da Grécia) e também colocou minas ao longo do litoral grego.

No oeste, o marechal-de-campo Wilhelm Keitel assinou uma ordem determinando o reforço da Sardenha.

Mesmo depois de iniciado o ataque principal à Sicília, os alemães continuavam pensando tratar-se apenas de uma manobra secundária. O êxito da missão pode ser avaliado nas palavras do marechal-de-campo, Erwin Rommel, cujos documentos pessoais revelam que, quando os aliados invadiram a Sicília, as defesas alemãs achavam-se dispersas em consequência do encontro do cadáver de um mensageiro diplomático nas costas da Espanha.

É óbvio que a Operação tinha muito mais detalhes do que os aqui mencionados, porém, nosso objetivo não é o detalhamento da Operação, mas mostrar a importância do Serviço de Inteligência e Contra-Inteligência para uma empresa, em particular a atividade de Contra-Inteligência, que se utiliza de meios valiosíssimos para garantir a sustentabilidade nesse mercado globalizado, agressivo e competitivo.

Joffre Coelho Chagas Junior

Mestre em Operações Militares - Escola de Aperfeiçoamento de Oficiais do Rio de Janeiro - RJ; especializado em Gestão de Segurança Empresarial pela FECAP - SP; Gestión de Seguridad Empresarial Internacional pela Universidad Pontificia Comillas de Madrid – Espanha; Bacharel em Ciências Militares, graduado pela Academia Militar das Agulhas Negras de Resende – RJ; Certificado de Especialista em Segurança - ABSO; Especializado em Investigação de Roubo de Cargas pela Academia de Polícia do Estado de São Paulo; Gerenciamento de Risco no Transporte Rodoviário de Cargas pela FECAP - Brasiliano & Associados; diversos cursos/seminários em Segurança, Criminalidade, Técnicas de Entrevistas e Gerenciamento de Riscos no Transporte de Cargas; Professor da FESP/FAPI/ Brasiliano & Associados; Gerente da Superintendência de Averiguação de Sinistro da Empresa GPS Logística e Gerenciamento de Risco (PAMCARY).

sumário

LER & SABER

Mariana Fernandez

O RISCO COMPENSA

Aqueles que desejam grandes recompensas precisam estar dispostos a correr riscos consideráveis. Esta é a proposta do escritor Aswath Damodaram, autor do livro **Gestão Estratégica do Risco** (Editora Bookman, 384 páginas).

O professor de Finanças também destaca, em sua nova obra, a questão do risco à inovação e avalia que muitas das mais valiosas e duradouras invenções, ao longo da história, surgiram do desejo de eliminar o problema, tendo que sair de posições cômodas e cautelosas em que um profissional se coloca quando confrontado. Um exemplo pode ser dado dentro de um campo de futebol. Um jogador bem preparado técnico e taticamente, assimila um companheiro de time, mesmo cercado por adversários. Ele ainda consegue ter uma visão geral do campo e dá o passe perfeito para seu companheiro. É o que destoa, nesse sentido, jogadores ordinários de jogadores renomados, como os brasileiros Ronaldinho Gaúcho e Kaká, o português Cristiano Ronaldo e o astro inglês David Beckham, avaliados em milhões de euros.

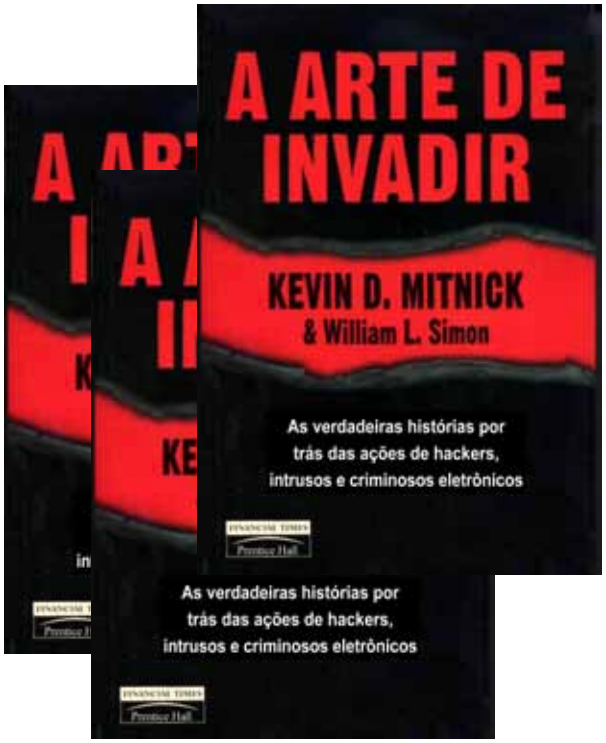
Um outro exemplo de como o risco compensa pode ser demonstrado pelos meios de comunicação e sua credibilidade, a principal fonte de investimento. Empresas e investidores buscam essa confiabilidade face à previsibilidade e certeza. No entanto, embora todos precisem estar cientes dessa idéia, torná-la foco de gestão de risco é um erro. O livro demonstra que não se deve misturar gestão de risco com limitação, restrição.

Aswath Damodaram delineia que uma atitude "irracional" frente ao risco se faz fundamental dentro do mercado competitivo. Pode-se explanar que investidores e companhias tentam tirar, incansavelmente, proveito dessa limitação, ainda que o assunto se torne corriqueiro dentro do campo acadêmico. Um caso que serve como destaque é o das finanças comportamentais. Esse novo campo de estudos, também conhecido como Economia Comportamental, contrapõe-se ao pressuposto de racionalidade dos tomadores de decisão adotado pelas Finanças Modernas.

Gestão Estratégica do Risco relata a situação em que os profissionais tendem a ficar desatentos e preguiçosos quando as coisas vão bem. Na maioria dos casos, isso resulta em excesso de confiança. "É exatamente esse tipo de desatenção que dá margem às grandes crises. A natureza humana não consegue se desvencilhar do ciclo de excesso de confiança seguido por frustração. Depois de abordar algumas formas de reação frente ao risco, meu livro busca descrever sistemas que podem ser usados para escapar desse comportamento típico", afirma o escritor, em recente entrevista à imprensa.

Por outro lado, o especialista reconhece que empresas que se expõem aos tipos errados de riscos podem sair-se ainda pior devido à precipitação. Quem busca desmistificar o risco de forma sucinta terá em mãos uma leitura amplamente precisa, direcionada ao profissional empreendedor e detalhada por um dos principais especialistas em finanças comportamentais.

QUANDO INVADIR SE TORNA UMA ARTE



Hackers, intrusos, criminosos eletrônicos... Na era maquiavélica pós-Marvel, Kevin D. Mitnick e William L. Simon - especialista em programação de softwares e escritor, respectivamente – oferecem, na obra **A Arte de Invadir** (Editora Pearson, 245 páginas), uma viagem sobre situações cheias de espiões, intrigas, suspense e desafios, baseada em fatos verídicos. De cassinos monitorados no mais alto padrão de segurança ao principal site do governo norte-americano, a dupla rege uma série de situações, carregada de vulnerabilidade, muitas vezes engraçada, que vai prender e orientar o profissional da área de TI a aprimorar seu respectivo sistema e trazer tranquilidade à sua organização.

Se você não é um profissional, mas gosta de histórias de crimes ousados, arriscados e que exigem sangue frio, a obra lhe propiciará horas agradáveis de uma leitura moderna, complexa em conhecimento, mas de fácil entendimento.

O livro descreve casos, por exemplo, em que a audácia, aliada a inteligência e a tecnologia, decifrou sistemas de videopoker em Las Vegas. Mulheres de mini-saias riem, bebem, chamam a atenção, enquanto uma câmera posicionada estrategicamente pelos 'criminosos' capta informações sobre o ciclo de tempo exato de uma máquina a ser hackeada pelo grupo.

Outra situação descrita é o encontro virtual entre jovens hackers, familiarizados ao computador desde a infância, e terroristas paquistaneses supostamente ligados ao líder da Al-Qaeda, Osama Bin Laden, interessados em invadir websites das Forças Armadas dos Estados Unidos. Segundo Mitnick, todo hacker é, de uma maneira ou de outra, um rebelde que vive padrões diferentes e adora vencer o sistema. Prato cheio àqueles que vislumbram derrubar conjuntos complexos de informação.

No coração de Londres, terra da rainha Elizabeth e do Big Ben, outro grupo de hackers habita um galpão sem janelas, no fundo de um edifício. Pessoas distantes da sociedade, não influenciadas pelo mundo exterior. Cada um trabalhando febrilmente em sua mesa, mas num clima bem descontraído. Queriam acessar a rede interna de uma empresa, que fazia grandes transferências em dinheiro.

Seguindo esses exemplos, a obra demonstra, em geral, como os hackers desvendam a fragilidade das redes e dos sistemas, usualmente configurados no ambiente de negócios. A experiência dos jovens demonstra o que sabem e como pensam; descreve o perfil de neo-intelectuais especializados em esmiuçar as mais complicadas redes de proteção. Assemelha-se a um jogo de xadrez, em que a superação se dá por meio de uma jogada mais inteligente do que a do adversário.

Os fatos servem de orientação aos projetistas e programadores, pois traz detalhes atualizados sobre prevenção tecnológica, mecanismos estes que servem de plataforma demonstrativa de que algo possa acontecer a um sistema de segurança. Permite, além, um vasto aprofundamento sobre o assunto, pois alerta contra futuras invasões cibernéticas.

Se você trabalha na área de segurança em sua organização e gosta de situações tensas, cheias de espiões e intriga da vida real, prepare-se para uma leitura excitante, ou melhor, prepare-se para uma aula.