ISSN 1678-2496N

b&a
BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

www.brasiliano.com.br | Janeiro 2011 | edição 62

Um Modelo de Análise de Risco para Desastres - RJ

ISPS CODE no maior porto da América Latina


equilíbrio
entre técnica X ousadia
178
109
42
A BRASILIANO & ASSOCIADOS analisa e avalia seus riscos, otimiza e oferece soluções.
Com a BRASILIANO & ASSOCIADOS sua empresa terá uma Gestão de Riscos Integrada.
b&a
BRASILIANO&ASSOCIADOS
info@brasiliano.com.br
www.brasiliano.com.br
11 5531 6171

Sumário




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.

Revisão | Ana Paula Deodato.

Edição, arte e Diagramação | Agencia BM Design

Colunista | Ana Paula Deodato.

Colaboradores desta edição | Bianca Padovani , Evaldo Tavares Barbieri, Jéssica Mary dos Santos , Leandro Jesus, Marcos Elias e Rodrigo Segura da Silva

Foto Capa | Valter Campanato/ABr

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

Negligência na Administração Pública: falta de processo estruturado de gestão de riscos

Em janeiro do ano passado, 2010, escrevi um editorial para nossa revista de número 51, abordando o mesmo assunto, ou seja a ineficiência e a falta de pró atividade dos gestores públicos com a questão das catástrofes naturais. Há 50 anos que o Brasil lida com o problemas dos deslizamentos e enchentes, tendo como causas sempre os mesmos fatores de riscos. O pior as soluções também!! Se não houver uma costura estratégica entre os três poderes federal, estadual e municipal, se nossa justiça continuar sendo omissa nas questões de ocupação do solo, se não houver uma política séria de habitação, a situação tende somente a piorar. Falta processos de prevenção e uma forte campanha educativa! Falta responsabilidade por parte dos governantes!

O início de 2011, de novo, foi repleto de desastres no Brasil, onde no Rio de Janeiro os deslizamentos e enchentes estão entre os 10 maiores do mundo, segundo dados da ONU. Fica clara a necessidade dos líderes empresariais e das instituições públicas focarem na gestão de riscos, com o foco preventivo e de crise, para poderem ter a capacidade da visão prospectiva – visão antecipatória - e na operacionalização de planos de respostas a emergência.

A visão prospectiva só é conseguida através de um processo estruturado de gestão de riscos. Hoje temos ferramenta e processos estruturados, tal como o framework sugerido pela ISO 31000, que inclui a compreensão do contexto estratégico tanto interno como externo, ou seja, a construção de cenários. Outra fase extremamente importante é a identificação e análise de riscos, onde o nível de criticidade dos eventos é projetado. Com isso, a instituição pública deve estruturar planos de respostas alinhados com o nível de criticidade.

Hoje no Brasil não é isso que estamos vendo. E pior, sempre as mesmas desculpas!! Nota-se claramente que não existe gestão de riscos e crise, o que faz com que estes eventos passem a ter um caráter somente reativo. E só na reação improvisada as dificuldades aumentam e são desordenadas. Quem paga a conta? A população que sofre, sendo vítima direta desta falta de responsabilidade dos gestores públicos. Isso é FATO e não hipótese!! Basta terem visto os noticiários do mês de janeiro de 2011.

Lendo a Revista Época número 661, de 17 de janeiro de 2011, no editorial da Diretora da Sucursal Rio de Janeiro, Ruth de Aquino, ela ressalta: “é preciso romper o círculo vicioso de tempestades. A omissão equivale ao assassinato”. Concordo plenamente, pois se o gestor público sabe, teoricamente, os riscos,

sua probabilidade e respectivos impactos, porque não trabalha na prevenção e contingenciamento? Preparo? Responsabilidade? Burrice? Crença que Deus é brasileiro? Cara de pau?

Agir já!! Essa é uma responsabilidade do gestor público de hoje, porque "o espírito de uma organização é criado a partir do topo. E se cai é porque o topo apodrece. Como diz o provérbio: as árvores morrem a partir do topo" (Drucker).

Será que temos o topo podre?? O que fazer?? Na minha opinião falta responsabilidade dos gestores, deveria haver punição séria, talvez só assim os gestores públicos acordassem!!

Bom 2011, se Deus deixar...

Boa leitura e sorte!!!

Antonio Celso Ribeiro Brasiliano
Publisher

abrasiliano@brasiliano.com.br

Audit Risk & Compliance

As áreas de Auditoria Interna, Controles Internos, Compliance, Gestão de Riscos Corporativos, e os seus respectivos Comitês e Responsáveis, representam hoje importantes pilares na prevenção, erradicação e combate às situações de descontrole, que permitem a ocorrência de prejuízos, fraudes e riscos, que podem comprometer seriamente a performance e a imagem das Organizações perante o mercado.

Nos últimos anos diversas novas leis e regulamentações têm sido divulgadas no sentido de refinar o papel desses importantes agentes e tornar cada vez mais efetiva a sua participação no que tange à precisa implementação e utilização de sistemas e controles que assegurem a otimização dos recursos.

Por esses motivos, os profissionais que atuam nessas áreas têm sido cada vez mais valorizados, requerendo-se, por outro lado, constante aperfeiçoamento da parte técnica e da capacitação dos envolvidos para responder a um nível de exigências e responsabilidades cada vez maiores.

Assim, integrando de maneira balanceada o repasse do conhecimento por meio de trabalhos de consultoria ou de cursos e treinamentos altamente especializados, a Brasiliano & Associados tem desempenhado importante papel na parceria e suporte àqueles que necessitam compartilhar estes desafios, aliando competência, prazo, qualidade e custos acessíveis.

Nossos serviços são independentes, com uma visão prospectiva, utilizando metodologias, ferramentas de tecnologia da informação e diversos outros recursos para viabilizar a atuação precisa em assuntos de tamanha relevância.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários assuntos, as quais podemos destacar nos seguintes principais serviços:

- Diagnóstico e Implantação de Áreas de Auditoria Interna e Compliance;
- Avaliação da Performance de Áreas/Equipes de Auditoria Interna e Compliance;
- Suporte à função de Compliance e Auditoria Interna;
- Terceirização Parcial ou Total da Função de Auditoria Interna e Compliance;
- Elaboração de Relatórios de Auditoria Interna;
- Suporte e Participação em Comitês de Auditoria Interna, de Compliance, de Controles Internos e de Gestão de Riscos;
- Redesenho de Processos de Negócios;
- Avaliação dos Processos e Sistemas de Controles Internos;
- Elaboração de Mapeamento de Riscos;
- Plano de Ação para Monitoramento de Riscos;
- Diagnóstico e Implementação de Auditoria Baseada em Riscos;
- Elaboração da Política da Auditoria Baseada em Riscos;
- Diagnóstico e Implementação de Auditoria Contínua;
- Diagnóstico para o Quality Assessment Review da Área de Auditoria Interna.

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

Foto: Vladimir Platonow/ABr

Um modelo de Análise de Riscos para Desastres

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

Introdução

No Brasil, os desastres naturais têm sido tratados de forma segmentada entre os diversos setores da sociedade. Nos últimos anos vem ocorrendo uma intensificação dos prejuízos causados por estes fenômenos devido ao mau planejamento urbano. Ações integradas entre comunidade e universidade são fundamentais para que os efeitos dos desastres naturais sejam minimizados. A universidade deve contribuir na compreensão dos mecanismos dos desastres naturais através do monitoramento, diagnóstico e modelagem. Estas informações devem ser repassadas à sociedade, que, de forma organizada, deve agir para minimizar os danos provocados pelos desastres. Num contexto local, sugere-se a criação de grupos comunitários capacitados para agir antes, durante e depois do evento, auxiliando assim os órgãos municipais de defesa civil.

Atualmente na escala mundial, cada R$ 1 investido em prevenção equivale, em média, entre R$ 25 e 30 de obras de reconstrução pós evento. Os desastres têm magnitudes amplas e variadas, fundamentalmente pela falta de alocação de recursos e pela escassez de textos que orientem para a fase de prevenção. Isso é um fato, que preocupa órgãos nacionais e internacionais e que prega por visar formação, treinamento e preparação pré-evento.

Conceito de Desastres Naturais

Utilizaremos o conceito do Livro Prevenção de Desastres Naturais, dos pesquisadores MASATO KOBIYAMA, MAGALY MENDONÇA, DAVIS ANDERSON MORENO, ISABELA P. V. DE OLIVEIRA MARCELINO, EMERSON V. MARCELINO, EDSON F. GONÇALVES, LETICIA LUIZA PENTEADO BRAZETTI, ROBERTO FABRIS GOERL, GUSTAVO SOUTO FONTES MOLLERI, FREDERICO DE MORAES RUDORFF, publicado pela editora Organic Trading, Curitiba, 2006.

"Inundações, escorregamentos, secas, entre outros, são fenômenos naturais severos, fortemente influenciados pelas características regionais, tais como, rocha, solo, topografia, vegetação, condições meteorológicas. Quando estes fenômenos intensos ocorrem em locais onde os seres humanos vivem, resultando em danos (materiais e humanos) e prejuízos (sócio-econômico) são considerados como "desastres naturais".

Segundo o Glossário de Defesa Civil: estudo de riscos e medicina de desastres, (1998), desastre é definido como resultado de eventos adversos, naturais ou provocados pelo homem, sobre um ecossistema (vulnerável), causando danos humanos, materiais e/ou ambientais e conseqüentes prejuízos econômicos e sociais. Aqui nota-se que o termo "adverso" significa hostil, inimigo, contrário, aquele que traz infortúnio e infelicidade.

"Inundações, escorregamentos, secas, entre outros, são fenômenos naturais severos, fortemente influenciados pelas características regionais, tais como, rocha, solo, topografia, vegetação, condições meteorológicas. Quando estes fenômenos intensos ocorrem em locais onde os seres humanos vivem, resultando em danos (materiais e humanos) e prejuízos (sócio-econômico) são considerados como "desastres naturais"


Foto: Valter Campanato/ABr

Os desastres são normalmente súbitos e inesperados, de uma gravidade e magnitude capaz de produzir danos e prejuízos diversos, resultando em mortos e feridos. Portanto, exigem ações preventivas e contingenciais, que envolvem diversos setores governamentais e privados, visando uma recuperação que não pode ser alcançada por meio de procedimentos rotineiros.

Os estudiosos de desastres sugerem de seis a sete itens que as instituições responsáveis pelo seu tratamento devem identificar:

1. estimar a área ocupada pelo ser humano nas áreas de perigo;
2. determinar a faixa de ajuste possível contra eventos extremos;
3. examinar como a população percebe os desastres naturais;
4. examinar os processos de seleção de medidas adequadas;
5. estimar os efeitos da política sobre essas medidas;
6. entender como aspectos socioeconômicos da sociedade contribuem à geração de desastres.

Os parâmetros para medição relacionados aos eventos naturais que estão diretamente vinculados aos desastres naturais são:

1. magnitude (alta – baixa);
2. freqüência (freqüente – rara);
3. duração (longa –curta);
4. extensão da área (ampla – limitada);
5. velocidade de ataque (rápida – lenta);
6. dispersão espacial (difusa – concentrada);
7. espaço temporal (regular – irregular).

Classificação de Desastres

Com relação à classificação, os Manuais da Defesa Civil, os classifica quanto à intensidade, a evolução, a origem e a duração.

a) Intensidade

Na proxima pagina mostra os **quadro 1** níveis de desastres em relação à intensidade, segundo Manual da Defesa Civil Brasileira.

Os níveis I e II são desastres facilmente superáveis pelo município, não havendo necessidade de recursos proveniente do estado ou da união. O nível III significa que a situação de funcionalidade pode ser restabelecida com os recursos locais, desde que complementados com recursos estaduais e federais. Neste nível, o município declara Situação de Emergência (SE). O nível IV significa que o desastre não é superável pelos municípios, mesmo quando bem informados e preparados. Nesta situação, ocorre a decretação do Estado de Calamidade Pública (ECP). Quando o município necessita de apoio do governo estadual ou federal, o município deve preencher o formulário de Avaliação de Danos e o envia com os demais documentos exigidos à Defesa Civil Estadual que homologa ou não a situação decretada pelo município.

quadro 1

Nível	Intensidade	Situação
I	Desastre de pequeno porte, onde os impactos causados são pouco importantes e os prejuízos pouco vultosos. (Prejuízo ≤ 5% PIB municipal)	Facilmente superável com os recursos do município.
II	De média intensidade, onde os impactos são de alguma importância e os prejuízos são significativos, embora não sejam vultosos. (5% < Prejuízo ≤ 10% PIB)	Superável pelo município, desde que envolva uma mobilização e administração especial.
III	De grande intensidade, com danos importantes e prejuízos vultosos. (10 % < Prejuízo ≤ 30% PIB)	A situação de normalidade pode ser restabelecida com recursos locais, desde que complementados com recursos estaduais e federais. (Situação de Emergência – SE).
IV	Com impactos muito significativos e prejuízos muito vultosos. (Prejuízo > 30% PIB)	Não é superável pelo município, sem que receba ajuda externa.Eventualmente necessita de ajuda internacional (Estado de Calamidade Pública – ECP).

O preenchimento do formulário AVADAN é o registro oficial de desastres no Brasil. De acordo com a Secretária Nacional de Defesa Civil (SEDEC), os desastres súbitos (agudos) geralmente caracterizam a situação de emergência e até o estado de calamidade pública, enquanto os desastres graduais (crônicos) não justificam na maioria dos casos a decretação, pois sua evolução permite realizar uma preparação e resposta ao desastre, o que pode reduzir os danos e prejuízos.

b) Evolução

Segundo o Manual de Defesa Civil, há três tipos de desastres relacionados a evolução. Os desastres **súbitos** são aqueles que se caracterizam pela rápida velocidade com que o processo evolui, por exemplo, as inundações bruscas e os tornados. Ao contrário do anterior, os **graduais** caracterizam-se por evoluírem em etapas de agravamento progressivo, como as inundações graduais e as secas. O outro tipo é a **Somação de efeitos parciais**, que se caracteriza pela ocorrência de numerosos acidentes semelhantes, cujos impactos, quando somados, definem um desastre de grande proporção. Por exemplo, acidentes de trânsito e de trabalho.

c) Origem

Este critério também se caracteriza por três tipos: os **naturais**, que são aqueles provocados por fenômenos naturais extremos, que independem da ação humana; os **humanos**, que são aqueles causados pela ação ou omissão humana, como os acidentes de trânsito e a contaminação de rios por produtos químicos; e os desastres **mistos** associados às ações ou omissões humanas, que contribuem para intensificar, complicar ou agravar os desastres naturais. É muito difícil ocorrer um desastre puramente natural. Quase todos os desastres recebem de

alguma maneira, uma influência antrópica. Assim, se olharmos por este prisma, existiriam somente desastres mistos.

d) Duração

Os desastres naturais são classificados em dois tipos: **episódicos e crônicos**. Geralmente os desastres denominados **episódicos** tais como terremoto, vulcanismo, tsunami, inundação e fluxo de detrito, chamam mais atenção por causa de sua magnitude. Entretanto, desastres **crônicos** tais como erosão do solo, geram sérios prejuízos ambientais, especialmente em longo prazo. A erosão do solo pode causar desertificação, degradação, assoreamento dos rios, entre outros, podendo resultar na incidência de mais eventos catastróficos, como escorregamentos e inundações.

Desastres no Brasil

Segundo a base de dados internacional sobre desastres da Universidade Católica de Louvain, Bélgica, entre 2000 e 2007 mais de 1,5 milhões de pessoas foram afetadas por algum tipo de desastre natural no Brasil. Os dados também mostram que, para este mesmo período, ocorreram no país cerca de 36 grandes episódios de enchentes, secas, deslizamentos de terra e o prejuízo econômico gerado por esses eventos é estimado em mais de US$ 2,5 bilhões.

Avalia-se que, no Brasil, os desastres naturais mais comuns são as enchentes, a seca, a erosão e os escorregamentos ou deslizamentos de terra. Eles são responsáveis por um número elevado de perdas humanas e materiais todos os anos.

Esses dados são corroborados através da pesquisa de Informações Básicas Municipais - MUNIC, realizada pelo IBGE em 2002 e publicada em 2005. Essa pesquisa, que enfoca a ótica do gestor municipal, mostra que, no Brasil, os maiores desastres relacionam-se a inundações, escorregamentos e erosão, e que esses processos estão fortemente associados à degradação de áreas frágeis, e são potencializados pelo desmatamento e por ocupações irregulares. Os dados revelaram que cerca de 50% dos municípios brasileiros declararam ter sofrido algum tipo de alteração ambiental nos 24 meses anteriores à pesquisa e, dentre esses, cerca de 16% sofreram com deslizamentos de encosta e 19% com inundações.

O desastre na Serra Fluminensa está catalogado entre os 10 maiores do mundo, com mais de 600 vítimas e 25000 desabrigados.

A **tabela 1** abaixo mostra nosso total despreparo ao longo dos anos

tabela 1

Ano	Local	Mortos	Desabrigados
1967	Rio de Janeiro	1000	5000
1967	Caraguatatuba – SP	436	3000
1987	Rio de Janeiro	292	20000
2008	Santa Catarina	135	54000
2010	Rio de Janeiro	283	11000
2011	Rio de Janeiro	600	35000

Pergunta: Há contingenciamento previsto? Por que sempre as autoridades são pegas de surpresa? Sempre será culpa da mãe natureza?

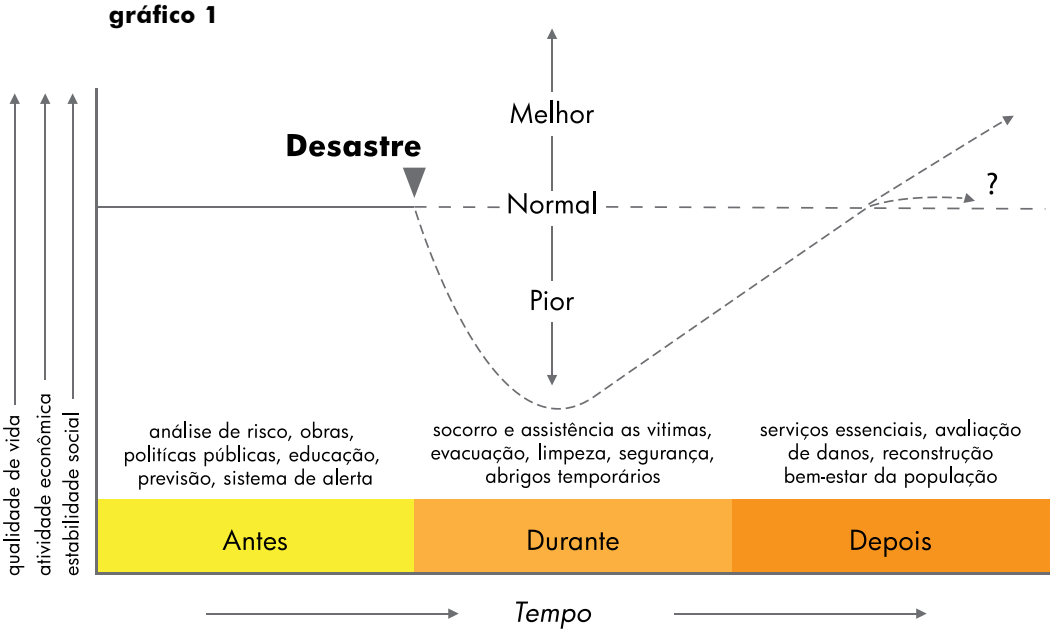
Fases do Desastres

Segundo o Coronel do Corpo de Bombeiros do Estado do Rio de Janeiro, Sérgio Baptista de Araújo, em seu livro Administração de Desastres, a administração de desastres se analisa e estuda para fins práticos, de forma sistemática como uma sequência cíclica de etapas que se relacionam entre si, e que se agrupam por sua vez em três fases distintas: antes, durante e depois.

No **gráfico 1** abaixo poderemos visualizar suas fases com as ações a serem desenvolvidas.

A base de qualquer Plano de Resposta a Emergência consiste na elaboração de uma Análise de Riscos, a qual é uma forma de se antever cenários e de se definir as medidas a serem implementadas, quer em termos de convivência com o risco, prevenção (diminuir a chance de ocorrência), ou intervenção (ação emergencial de controle).

gráfico 1



Processo de Gestão de Riscos para Desastres

Um dos objetivos fundamentais da Gestão de Riscos em Desastres é a prevenção de riscos coletivos e a ocorrência de acidente grave ou de catástrofe, exercendo-se a sua atividade em diversos domínios como o levantamento, previsão, avaliação e prevenção dos riscos coletivos; a análise permanente das vulnerabilidades perante situações de risco e a informação e formação das populações, visando a sua sensibilização em matéria de autoproteção.

Assim, a caracterização do risco é um fator fundamental no âmbito das atividades da Gestão de Riscos para Desastre, contribuindo para os objetivos do planejamento de emergência, ao prevenir ou minimizar situações de risco e atenuar os seus efeitos.

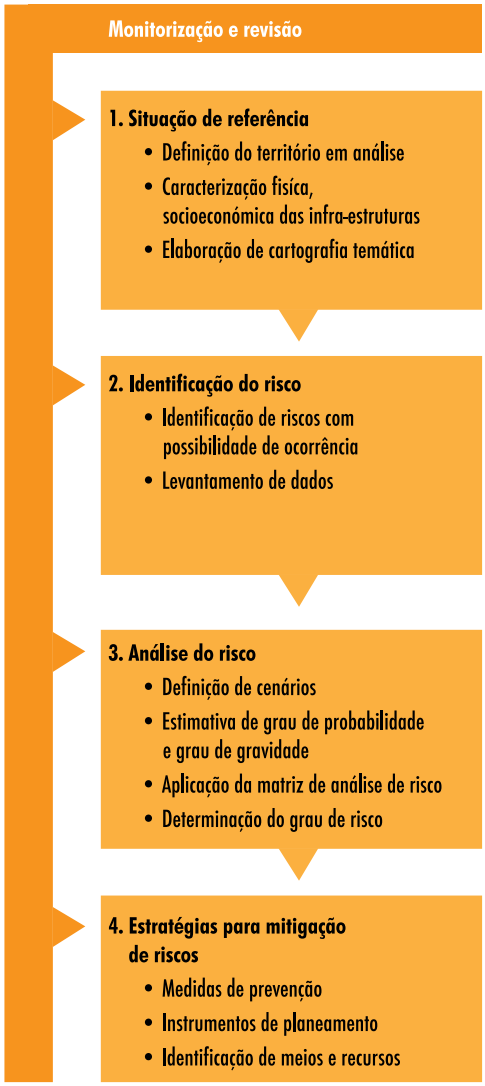
A vantagem da utilização de um processo de caracterização de risco, no âmbito do planejamento de emergência, é que oferece a oportunidade para:

- proporcionar um melhor conhecimento do risco

- promover a tomada de decisão sobre o risco e alocação de recursos;
- reduzir os graus de risco para a população, os bens ou o ambiente;
- enfatizar as atividades de prevenção e mitigação do risco.

O processo que se apresenta neste artigo é uma sugestão e pretende auxiliar as instituições públicas e privadas que necessitam elaborar uma caracterização de risco no âmbito das suas atividades. Porque existem contextos diferentes, estas orientações devem ser adaptadas para as circunstâncias específicas em que são utilizadas, consoante as áreas territoriais em análise.

figura 1



Caracterização do Risco

O processo de caracterização do risco tem como objetivo aumentar o conhecimento dos fatores de risco que afetam o território, identificando a sua localização, gravidade dos danos potenciais e probabilidade de ocorrência.

O processo deverá iniciar-se com a definição da situação de referência e com a identificação e análise dos riscos com potencial para causar danos em pessoas, bens ou ambiente. Concluída a identificação dos riscos, será necessário efetuar a sua análise e definir as medidas de prevenção e proteção a implementar. Deste modo, ao longo deste processo terá de se considerar a tipologia das ocorrências, a sua probabilidade de ocorrência e os danos expectáveis, de modo a estimar de que forma o evento pode afetar o território e qual a vulnerabilidade deste face ao risco em causa.

Na **Figura 1** ao lado, apresenta-se um resumo do processo de caracterização de risco que pretende dar resposta às seguintes questões:

- Que riscos podem afetar o território?
- Que consequências resultam da manifestação do risco?
- Qual a estimativa da população que pode ser afetada?

Situação de Referência

Esta etapa tem por objetivo introduzir as questões que se antecipem de maior relevância na análise à zona de estudo. Inclui-se nesta etapa a caracterização e a análise dos descritores mais importantes da área para a qual a avaliação do risco se encontra a ser desenvolvida e a forma


Foto: Wilson Dias/ABr

como esta poderá ser afetada na sequência de um acidente grave ou catástrofe.

Deste modo, a equipe de trabalho deve refletir sobre os aspectos relevantes do território,considerando a situação atual e futura, abrangendo por exemplo, aspectos de enquadramento administrativo, extensão territorial, contexto histórico, patrimonial e cultural.

O tipo de dados a recolher nesta etapa terá como objetivo a caracterização física, socioeconômica e de infra-estruturas, sendo por isso conveniente estabelecer contactos com as entidades que possam fornecer informações relevantes para este processo.

Caracterização física

Deverão ser abordados os aspectos biofísicos, nomeadamente os relacionados com geologia, clima (temperatura, precipitação, umidade relativa, vento, insolação, frequência de fenômenos adversos tais como nevoeiro, geada ou granizo), recursos hídricos (hidrografia, hidrologia, qualidade da água), qualidade do ar e uso do solo (cobertura vegetal,ordenamento e ocupação) por exemplo.

Nesta caracterização devem ser dadas respostas às seguintes questões:

- existem locais que contribuam para a fragilidade das pessoas, bens e ambiente?
- existem áreas sensíveis do ponto de vista ambiental, como sejam áreas protegidas ou vulneráveis?

Caracterização sócio - econômica

Deverá ser feita uma análise das dinâmicas demográficas e econômicas. As dinâmicas demográficas devem incluir a análise da população residente e flutuante por divisão administrativa, a densidade populacional, a estrutura etária e o número de alojamentos e edifícios. As dinâmicas econômicas devem incluir a análise da estrutura econômica, abordando o tecido empresarial e os setores de atividade mais representativos na área territorial do plano. Nesta caracterização devem ser dadas respostas às seguintes questões:

- Como estão as diversas comunidades geograficamente distribuídas? A ocupação é urbana, rural ou dispersa?
- Existem grupos particularmente vulneráveis, como um elevado número de idosos ?
- Há eventos durante os quais existe um elevado afluxo de pessoas? Realizam-se feiras agrícolas, festivais de música ou festividades religiosas com elevada participação de público?
- A população tem experiência em lidar com diferentes tipos de emergência? Por exemplo, a área em estudo é afetada por cheias

e a população adota medidas de auto-proteção?

Caracterização das infra-estruturas

A caracterização das infra-estruturas prende-se com a análise das estruturas que, pela sua importância numa operação de proteção civil, poderão ser consideradas sensíveis e/ou indispensáveis para a prevenção, planejamento e socorro. Como exemplo, podem considerar-se a rede viária (rodo e ferroviária), telecomunicações, abastecimento de água, eletricidade, combustíveis, portos, aeroportos, patrimônio, instalações dos agentes de proteção civil e hospitais, entre outras.

Com a identificação e localização destas infra-estruturas, e após delimitação dos locais onde os riscos podem ocorrer, é possível planejar, em função do tempo de reposta, a alocação de meios materiais e humanos em situação de emergência. Isto permite, em termos de prevenção, dotar os locais mais sensíveis com os meios de resposta necessários para minimizar a probabilidade de ocorrência e as respectivas consequências.

Nesta caracterização devem ser dadas respostas às seguintes questões:

- Como estão geograficamente implantadas na região as infra-estruturas de transporte (rodoviário, ferroviário, aéreo, marítimo), os serviços públicos, as empresas, etc.?
- Quais os pontos considerados críticos, ou seja, aqueles cuja interrupção do normal funcionamento afeta diretamente a sociedade (por exemplo uma subestação elétrica, hospitais ou equipamentos de defesa e segurança)?
- Quais as infra-estruturas que assumem papel relevante nas operações de proteção civil?
- Onde estão localizadas as centrais de comunicação, postos de abastecimento de combustível, etc.?
- Quais os locais com presença de substâncias perigosas e qual a sua localização relativamente à população e às áreas ambientalmente sensíveis, caso existam?


Foto: Valter Campanato/ABr

Cartografia

Os dados de caracterização do território deverão ser representados em tabelas e sob a forma de cartografia temática. Os elementos cartográficos devem incluir as referências cartográficas susceptíveis de serem utilizadas quer em fase de emergência quer em fase de reabilitação, incluindo cartas especializadas, como cartas geológicas, agrícolas, florestais, hidrográficas, zonas de risco de inundação, infra-estruturas sensíveis, risco de incêndio florestal, etc.

Articulação Política

A efetiva mitigação dos desastres não ocorre sozinha. Ela é criada, ou seja, é mais ainda criada pelo trabalho duro entre as organizações governamentais, buscando reduzir a perda de vidas e propriedades em decorrência dos desastres. A articulação política deve basear-se fundamentalmente no chamamento à consciência dos setores políticos para com o problema. A administração governamental, que provê as oportunidades

e obrigações no planejamento da mitigação dos desastres, deverá estar integrada com os três níveis da administração pública: municipal, estadual e federal. Portanto há a necessidade de saber claramente qual é o nível que o município possui de integração com estas esferas da administração pública.

Identificação de Riscos

A Identificação do Risco tem por objetivo localizar, e registrar as características dos principais riscos com possibilidade de ocorrência no território em análise.

No âmbito do planejamento de emergência de proteção civil, risco é definido como a probabilidade de ocorrência de um processo (ou ação) perigoso e respectiva estimativa das suas consequências sobre pessoas, bens e ambiente. Ou seja, seguindo a ISO 31000, temos que identificar seus fatores de riscos para podermos estimar a probabilidade e estimar a extensão do evento, suas conseqüências.

Os riscos podem ser agrupados na queles descritos na sua origem, em 3 grupos:

- Riscos Naturais, os que resultam do funcionamento dos sistemas naturais (sismos, movimentos de massa em vertentes, erosão do litoral, cheias e inundações);
- Riscos Humanos e ou Tecnológicos, os que resultam de acidentes, frequentemente súbitos e não planejados, decorrentes da atividade humana (cheias e inundações por ruptura de barragens, acidentes no transporte de mercadorias perigosas, emergências radiológicas);
- Riscos Mistos, os que resultam da combinação de ações continuadas da atividade humana com o funcionamento dos sistemas naturais (incêndios florestais).

Nesta etapa, as entidades responsáveis pela elaboração dos Planos de Emergência de Proteção Civil deverão listar os riscos potenciais, recorrendo a levantamento de dados de campo (por exemplo, a cartografia dos locais inundados na última cheia), a registros históricos (por exemplo, deslizamentos na última década) ou a estudos científicos (por exemplo, o estudo para determinar a susceptibilidade à liquefação de solos).

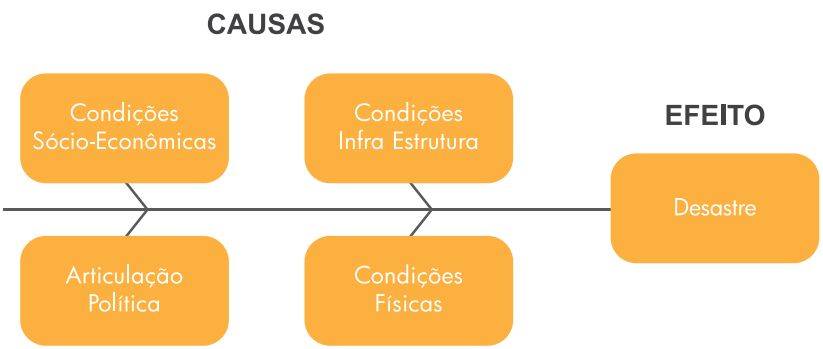
A caracterização de perigo e do risco deve ser consistente com os dados disponíveis, e ser suficientemente vasta para incluir um intervalo de opções que permita a redução do risco.

A listagem dos riscos deve ser elaborada utilizando a técnica do braisntorming, com uma equipe multidisciplinar do município, com base nas levantamentos da situação de referência: caracterização física, sócio-econômica, infra-estrutura e cartografia.

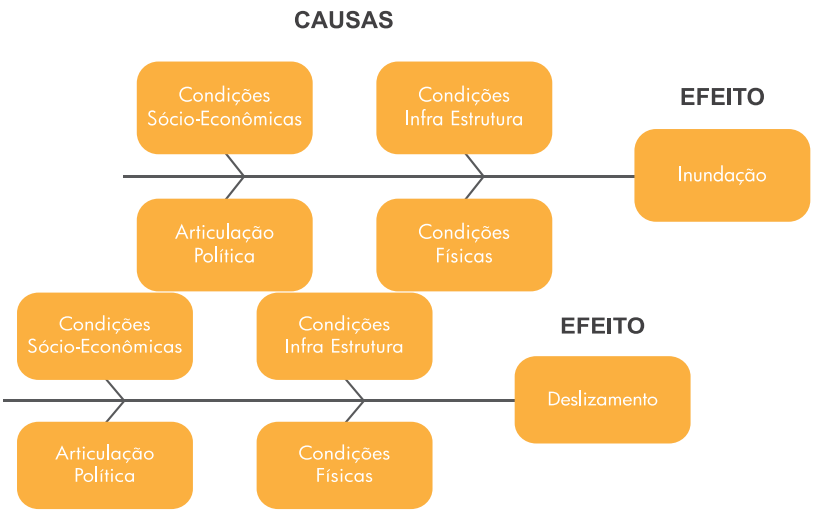
Fatores de Riscos

O ponto crucial da identificação dos riscos, seguindo o processo da ISO 31000 é o levantamento dos fatores de riscos, empregando uma ferramenta. Para isso sugerimos que empregue-se o **Diagrama de Causa e Efeito** adaptado para Desastres, com as quatro macro causas.

Diagrama de Causa e Efeito



As macro causas do diagrama de causa e efeito são frutos da referência da situação, ou seja fruto do diagnóstico realizado no território estudado. Nesta etapa estamos identificando de forma objetiva os fatores de riscos que contribuem para a concretização do desastre em estudo. Para cada tipo de desastre identificado há a necessidade de elaborar um diagrama de causa e efeito visando a objetiva identificação dos fatores de riscos.



Motricidade dos Fatores de Riscos – Matriz SWOT

Após a identificação dos vários fatores de riscos dos desastres, o administrador público precisa enxergar, de forma estratégica, quais são os fatores comuns a todos os eventos identificados e quais são os mais motrizes. Ou seja quais são os que podem de fato potencializar os desastres identificados.

Sugerimos a utilização da ferramenta gerencial denominada de Matriz SWOT, amplamente utilizada pelos gestores em planejamento estratégico, para identificar os pontos fracos, fortes, oportunidades e ameaças do contexto empresarial. A Matriz SWOT - FOFA, que em inglês significa SWOT - Strengths - Weaknesses - Opportunities – Threats e em português – Força – Oportunidade – Fraqueza - Ameaça. A avaliação das forças e fraquezas dizem respeito as condições dos sistemas e processos preventivos, ou seja processos que o município possui domínio de ação e decisão. São os chamados Fatores de Riscos Internos, variáveis internas. Os fatores de riscos considerados incontroláveis dizem respeito a ambiência externa, podendo ser negativa – Ameaças e ou positivas – Oportunidades. A matriz possui quatro células, avaliadas quantitativamente, utilizando-se dois parâmetros:

a) **Magnitude** significa o tamanho ou grandeza que o fator de riscos possui perante o contexto estudado do município. Caso aconteça, positivamente ou negativamente, o quanto ela vai influenciar neste o contexto. A magnitude é ranqueada, utilizando-se uma pontuação, que varia de –3 a +3, dentro do seguinte parâmetro: + 3 (alto); + 2 (médio);+ 1 (baixo), para cada elemento positivo (força ou oportunidade) e –1 (baixo); -2 (médio); -3 (alto) para cada variável negativa (fraqueza e ameaça). No nosso caso podemos ter como parâmetro para poder dar a nota da magnitude na célula da fraqueza e ameaça o número de vezes que as variáveis aparecem no diagrama de causa e efeito. É uma forma mais objetiva de saber a magnitude do Fator de Risco, pois se um Fator de Risco aparece 5 vezes em seis eventos estudados, significa que esta variável é de "grande"magnitude.

b) **Importância** significa a prioridade que esta variável deve possuir perante a conjuntura da empresa. É uma nota subjetiva com base na experiência da equipe que está avaliando. Utilizamos também três níveis de pontuação: 3 (muito importante); 2 (média importância); 1 (pouca importância). Neste caso, não há contagem negativa , pois o critério Importância sempre é positivo

Ressaltamos que esta ferramenta já vem sendo aplicada em estudos de Gestão de Riscos nos últimos dez anos, pela Brasiliano & Associados e seu resultado tem demonstrado de grande valia. Outro ponto importante é que está alinhada com a ISO 31000, onde pede ferramenta para avaliar a motricidade dos fatores de riscos.

Matriz FOFA - Brasiliano & Associados

Para ranquear os itens em cada célula, podemos multiplicar a avaliação da magnitude e da importância. Os fatores de riscos ranqueados com maior numeração, positiva e negativa, são considerados motrizes. Motrizes porque devem receber maior atenção. A matriz SWOT - FOFA demonstra o conjunto de Fatores de Riscos (Fraquezas e Ameaças), e seus pontos fortes e oportunidades. Com esta fotografia o administrador público enxergará seus pontos de maior fragilidade. Se formos observar sob o ponto de vista das fraquezas e ameaças contidas na Matriz SWOT, podemos afirmar que a Matriz SWOT é um resumo de todos os diagramas de causa e efeito, sem listar os fatores repetidos.

Análise de Riscos

Concluída a identificação dos riscos susceptíveis de afetar o território, é necessário efetuar a análise dos riscos considerados significativos para definição de medidas de prevenção, proteção e socorro. Nesta etapa, cada entidade deverá proceder ao registro de cada risco identificado, mantendo desta forma atualizada a informação relativa aos riscos e respectivas gravidade e probabilidade.

O método proposto para a análise do risco é baseado nos cenários de acidente associados a cada risco identificado e aplicação de uma matriz de risco com base na estimativa do grau de gravidade dos danos potenciais e na probabilidade de ocorrência do risco.

Neste âmbito, a probabilidade é definida como potencial frequência de ocorrências com consequências negativas para a população, ambiente e sócio economia e a gravidade é definida como as consequências de um evento, expressas em termos de

"Um cenário é uma representação simplificada da realidade com a função de ajudar a compreender os problemas e a gravidade dos mesmos"

escala de intensidade das consequências negativas para a população, bens e ambiente. Associado ao grau de risco (probabilidade x gravidade) está o conceito de vulnerabilidade ou fragilidade, a qual pode ser definida como o potencial para gerar vítimas, bem como perdas econômicas para os cidadãos, empresas ou organizações, em resultado de uma dada ocorrência.

Cenários

Um cenário é uma representação simplificada da realidade com a função de ajudar a compreender os problemas e a gravidade dos mesmos. Num plano de emergência os cenários destinam-se a descrever a progressão hipotética das circunstâncias e dos eventos, visando ilustrar as conseqüências dos impactos, mas especialmente a concepção das decisões e das operações de emergência.

A construção de cenários deve ser realizada para os riscos identificados previamente, tendo em conta os potenciais impactos dos eventos estudados. Deve-se ponderar uma multiplicidade de fatores na seleção da lista de cenários, os quais devem ser escolhidos por forma a testar a dimensão da resposta e os recursos necessários, em termos de quantidade, qualidade e oportunidade. Também é importante levar em consideração o potencial para a escalada de um evento ou o "Efeito Dominó" quando combinado com outros perigos, ou seja os impactos cruzados.

Os cenários deverão ser representados com recurso a cartas ou esquemas, de modo a constituírem uma visão global e a identificação e gestão eficiente das áreas prioritárias de intervenção.

Parâmetros e Critérios

Grau de Probabilidade - GP

Optamos por um processo para determinar o Grau de Probabilidade chamado de Lógica Intuitiva. Lógica Intuitiva é um processo estruturado e leva em consideração a expertise e experiência da equipe que está realizando o estudo.

O **GP** possui dois critérios: O **Critério dos Fatores de Riscos – FR** e o **Critério da Exposição - E**. O **GP** está alicerçado em uma fórmula simples, que calcula de forma direta, através da multiplicação dos dois critérios, o nível de possibilidade do evento vir a acontecer, frente à condição existente. Frente aos Fatores de Riscos identificados no diagrama de causa e efeito de cada risco. O Grau de Probabilidade – **GP** é a conseqüência da multiplicação dos fatores de riscos versus o critério da exposição. É uma multiplicação direta, onde cada critério possui uma escala de valoração 1 a 5.

Critério do Fator de Riscos – "FR"

Este critério possui quatro sub critérios, estudados na fase da identificação dos riscos. Os sub critérios possuem uma escala de valoração que mede o grau de influência para a concretização do perigo. Neste caso julgamos qual o nível de influência, por sub-critério, para que o perigo seja concretizado. É uma nota subjetiva, com base no diagrama de causa e efeito. Ou seja, a nota deve estar coerente com o diagrama de causa e efeito realizado. Em cada macro fator o gestor deverá realizar uma análise para verificar qual será o nível de influência daquele Macro Fator na concretização do perigo estudo. O gestor também deve olhar a Matriz SWOT, com o objetivo de verificar o grau de motricidade dos fatores de riscos dentro daquela macro causa. Por exemplo

no diagrama abaixo, digamos que na macro causa Infra Estrutura os fatores eletricidade e hospitais tiveram grau -9 da Matriz SWOT e Corpo de Bombeiros -6. Qual nota poderíamos dar, na escala de 1 a 5,de influência na potencialização do perigo de deslizamento? Deverá ser pelo menos 4 ou 5. Seria incoerente dar uma nota 2 ou até 3. Porque? Como podemos dar uma nota 3, que é média, se dos três fatores listados, temos dois com grau máximo. Portanto a Matriz SWOT passa a ser um balizador para o gestor na análise do nível de influência.

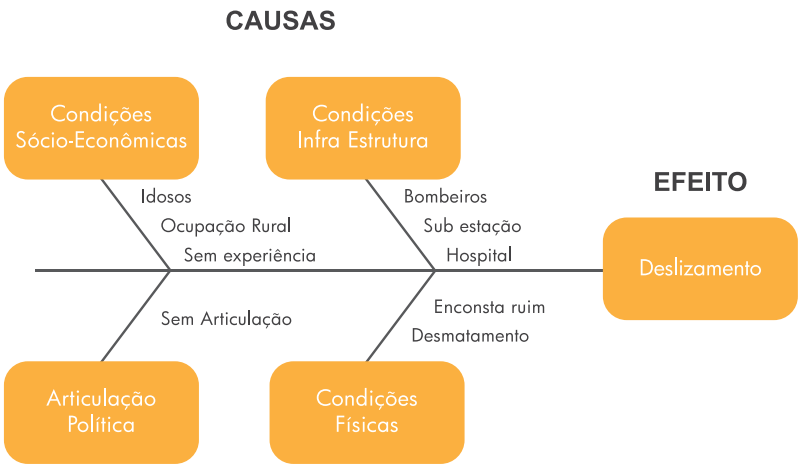


Tabela 2

Nível do Fator de Risco	
Escala	Pontuação
Influencia Muito	5
Influencia	4
Influencia Medianamente	3
Influencia Pouco	2
Influencia Muito Pouco – quase nada	1

Os quatro Macro Fatores de Riscos, que compõem o diagrama de causa e efeito, são uma sugestão, podendo variar de acordo com a complexidade do estudo. A **Tabela 2** ao lado valora a escala.

Após o estudo e análise pontuamos Cada Macro Fator, efetuando a soma do resultado e dividindo por quatro. Porque quatro? Por que existem quatro macro fatores. Se forem cinco macro fatores? Dividimos por cinco. Fazemos então o exercício:

$$FR = \frac{AP + CF + CIE + CSE}{4}$$

Legenda

DESASTRES

AP= Articulação Política

CF= Condição Física

CIE= Condição de Infra Estrutura

CSE= Condição Sócio Econômica

Critério da Exposição – E

Assim como no tópico anterior, o critério de exposição possui uma escala de valoração que mede a freqüência que os desastres costumam manifestar-se na região ou em regiões similares, com as mesmas características. Ponto importante é avaliar sob três óticas: as condições passadas, presentes e futuras. Não deve nunca, olhar somente o passado. Se o gestor olhar somente a freqüência com foco no passado ele estará fazendo uma projeção, não levando em consideração as variáveis presentes e futuras. Será um grande erro estratégico. A **tabela 3** na proxima página sugere a valoração.

Grau de Probabilidade – GP

O GP é o resultado da multiplicação do valor final do fator de risco versus o critério da exposição, conforme demonstrado abaixo:

GP = FR x E

Tabela 3

Critério da Exposição	
Escala	Pontuação
Uma vez por ano ou mais	5
Uma ou mais vezes pelo período entre 5 e 20 anos	4
Uma ou mais vezes pelo período entre 21 e 50 anos	3
Uma ou mais vezes a cada 100 anos	2
Uma ou mais vezes a cada 500 anos	1

Tabela 4

Escala	Nível de Probabilidade	
1 - 5	Baixa	4% a 20%
5,01 - 10	Média	20,01 a 40%
10,1 - 15	Alta	40,01 a 60%
15,01 - 20	Muito Alta	60,01 a 80%
20,01 - 25	Elevada	80,01 a 100%

Tabela 5

Escala	Área Afetada m2 (3)	Prejuízo Em US$ (2)	Desabrigados (4)	Vítimas Fatais (5)
1	0 – 369	10 - 103	1 – 148	1 – 20
2	370 – 2729	103 - 105	149 – 1096	21 – 148
3	2730 – 20171	105 - 107	1097 – 8103	149 – 1096
4	20172 – 149047	107 - 109	8104 – 59874	1097 – 8103
5	>149048	> 109	> 59875	> 8104

Tabela 6

Grau de Impacto	Nível de Impacto
4,51 – 5,00	Catastrófico
3,51 – 4,50	Severo
2,51 – 3,50	Moderado
1,51 – 2,50	Leve
1,00 – 1,50	Insignificante

Esta multiplicação direta representa o grau de probabilidade, sendo que o valor máximo obtido é 25, com a classificação dividida em cinco níveis. Para transformar esta classificação subjetiva em uma classificação objetiva, basta multiplicar pelo fator 4. Por que fator 4? Porque estamos fazendo uma equivalência entre o número máximo obtido na multiplicação direta entre os dois fatores (fator de riscos x fator de exposição) que é 25 e a porcentagem da probabilidade máxima que é 100%. Desta forma temos a **tabela 4** ao lado.

Verifica-se que sempre teremos um risco residual de 4%.

Critério do Impacto – Magnitude das Consequências

Para mensurar o impacto de um desastre, temos que levar em conta os seguintes fatores (**tabela 5**).

Obs: Tabela adaptada da Apostila Administração de Desastres, do TC Bombeiro Sérgio Baptista de Araújo.

O Nível de Impacto é o resultado da soma dos resultados de cada fator de impacto (multiplicação do peso versus a nota), dividido pela soma dos pesos, conforme demonstrado abaixo:

$$\text{Nível de Impacto} = \frac{\text{Área Afetada + Prejuízo + Desabrigados + Vítimas Fatais}}{\text{14 (soma dos pesos 3+2+4+5)}}$$

O nível de impacto possui a seguinte classificação (**tabela 6**).

Matriz de Riscos

Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento de cada desastre, o resultado da avaliação dos riscos será apresentado em

um mapa de riscos (**Matriz de Riscos**), permitindo o acompanhamento da dinâmica dos riscos. A matriz de riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Desta forma, pela divisão da matriz em quatro níveis de criticidade podemos avaliar o nível de vulnerabilidade da comunidade. Quanto maior for à probabilidade e o impacto de um desastre, maior será o nível de fragilidade. Os desastres plotados em cada nível terão um tratamento específico.

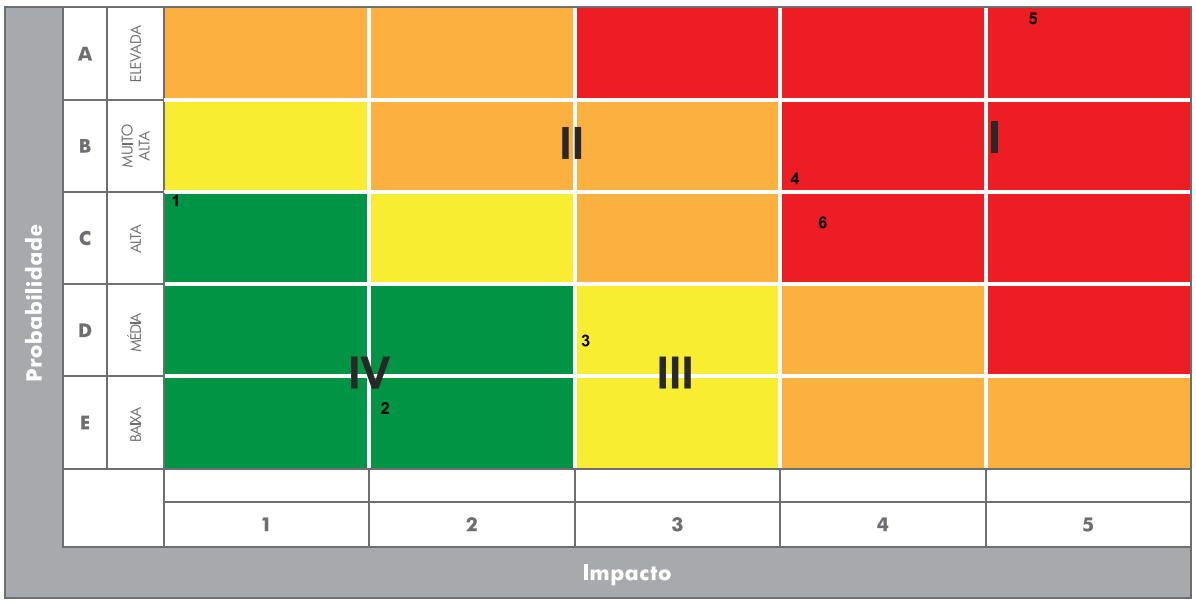
Desta forma poderemos priorizar as ações de contingência e de prevenção na comunidade estudada.

Estratégias de Mitigação dos Desastres – Plano de Ação

Após a identificação do grau de risco, são tomadas as decisões sobre as estratégias a implementar para a sua mitigação. Mitigação de risco pode ser definida como "qualquer ação sustentada para reduzir ou eliminar os riscos a longo prazo para as pessoas e os bens, dos perigos e os seus efeitos".

O ideal é que o Brasil tivesse uma legislação que obrigasse os municípios a terem um Processo de Gestão de Riscos, com a operacionalização dos respectivos Planos de Ação. A adoção de projetos ou de programas integrados destinados a mitigar os

Matriz de Riscos



LEGENDA						
PROBABILIDADE	5	B	B	A	A	A
	4	C	B	B	A	A
	3	D	C	B	A	A
	2	D	D	C	B	A
	1	D	D	C	B	B
		1	2	3	4	5
		IMPACTO				

NIVEIS DE TRATAMENTO	
A	Ação Imediata
B	Ação média e a curto prazo
C	Monitoramento e Gestão
D	Risco controlável

riscos e as vulnerabilidades do território é fundamental para que se obtenham resultados na eliminação ou na redução da possibilidade de ocorrência ou dos efeitos que possam eventualmente resultar de acidente grave ou catástrofe. As estratégias para mitigação de risco incluem diversos instrumentos como, por exemplo, a implementação de medidas no âmbito do ordenamento do território. Estas poderão ser consideradas como instrumentos de mitigação do risco através da regulação das áreas de risco ou da previsão de requalificação dessas áreas.

Outras medidas podem ser a implementação de sistemas de alerta e aviso; sensibilização da população; elaboração de planos de emergência de proteção civil; ou a realização de exercícios e simulados.

Conclusão

Os sistemas de respostas de emergência como um todo ainda não estão adaptados a situações de massa, pelos mais diversos fatores, tais como: problemas de comando, coordenação e organização do local do evento, dificuldade de comunicações e de suporte logístico ao local do evento. Um bom exemplo do fato foi demonstrado no terremoto da Cidade do México em 1984, quando os veículos de socorro que primeiro chegavam aos locais, especialmente as ambulâncias, se viam impossibilitadas de sair, em virtude da chegada de novos socorros, causando um autêntico "engarrafamento de viaturas de socorro".

O cenário do grande acidente mais o estresse e as dificuldades para se gerenciar a nova situação fazem com que as condições de trabalho se transformem em quase caóticas. As condições de pressão, a existência de múltiplos intervenientes, a polícia, as companhias de gás, luz, limpeza, as autoridades presentes, a imprensa, etc... Exigem uma nova organização de socorro para esses casos. Por essa razão, a previsão das consequências, com suas respectivas extensões é o principal fator-chave de sucesso de um Plano de Resposta a Emergência.

A base dessa previsão é o Processo de gestão de Riscos.

Infelizmente, ainda teremos inúmeros eventos sendo negligenciados pelos administradores públicos e privados, pela simples falta de operacionalização de processos estruturados de gestão de riscos.

No próximo artigo estaremos fazendo o Estudo de Caso Prático sobre a Serra Fluminense, empregando esta metodologia. Vai ficar claro a negligência dos administradores públicos.

Information Risk Assessment - IRA

As empresas enfrentam, hoje, desafios em várias frentes, tais como consumidores exigentes, regras cada vez mais complexas, novas regulamentações e o mercado cada vez mais competitivo.

A fuga de informações estratégicas e o roubo de documentos corporativos é hoje uma ameaça real. Segundo a Câmara de Comércio Americana dos EUA, os custos com a perda de propriedade intelectual giram em torno de US$ 25 bilhões de dólares. E o pior é que estas informações estratégicas não estavam armazenadas em computadores, mas disponíveis em recipientes de lixo, jogados em copiadoras, impressoras e nas mesas dos executivos e gerentes.

A fuga e ou roubo de informações estratégicas, por não proteger adequadamente e não saber elimina, por exemplo dados financeiros de cliente, podem resultar na responsabilidade direta de violação de privacidade. Ou seja as empresas podem ser processadas a indenizar seus clientes pela fuga e ou roubo de informações!

Acreditamos que no mercado brasileiro ainda exista muito o que fazer em termos de prevenção de fuga e roubo de informações estratégicas.

A Brasiliano & Associados avalia as fragilidades do ambiente, foco no Fator Humano, identificando o nível de risco da Fuga e ou Roubo de Informações Estratégicas. Tudo isso através de um processo prático e objetivo.

Oferecemos um trabalho independente, com uma visão prospectiva, utilizando metodologia própria, levando em consideração a informação exposta, o acesso aos documentos estratégicos, os equipamentos que contém informações e não estão devidamente protegidos e a infra estrutura física.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Gestão de Risco de Fuga e Roubo de Informações Estratégicas
- Mapeamento, Avaliação e Respostas aos Riscos
- Políticas de Segurança da Informação
- Programas de Sensibilização – Trato das Informações Estratégicas
- Programas de Inteligência e Contra Inteligência Empresarial
- Programas e Processos de Eliminação de Informações Estratégicas
- Avaliação das Fragilidades – Nível de Risco – Testes Operacionais

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

ISPS CODE no maior Porto da América Latina

*Evaldo Tavares Barbieri**

Resumo

ISPS CODE no Brasil medidas criadas pelo EUA para evitar a exposição dos terminais portuários ao terrorismo ao redor do mundo, facilitando também as exportações para os americanos que certamente sem a adoção desse código de segurança poderá haver barreira como os produtos exportados.

Palavras-chave: ISPS CODE, scanner, terminais portuários, exportação, terrorismo, risco, EUA.

Abstract

The procedures made by USA to avoid ISPS CODE in Brazil against exposure terrorism in port and ship around the world making better export for USA certainly without this security code could have barrier with the export products from Brazil to USA and others countries.

Keyword: ISPS CODE, scanner, port ship, export, terrorism, risk, EUA.

Introdução

O ISPS CODE (International Ship and Port Facility Security) é o código internacional de proteção de navios e instalações portuárias, que foi criado pós 11 setembro, com a finalidade de criação de medidas para mitigar os riscos que os países membros da SOLAS (Safe of Life at Sea) salvaguarda da vida

no mar e da IMO (International Maritime Organization) Organização Marítima Internacional onde a proposta era de que todos os portos integrante dos países membros teriam que estar com declaração de cumprimento das normas do ISPS CODE em julho de 2004, porém nos portos do Brasil as ações para a implementação não foram implantadas na data combinada, foram gastos milhões, mas somente no final do segundo semestre de 2010 que o porto de Santos recebeu seu documento que homologa como porto dentro das condições seguras para receber cargas e exportar cargas para os países membros.

Objetivo

Tem como objetivo focar nossos esforços na direção de melhor entender sobre a segurança portuária e o ISPC DODE, logicamente que não é desejo único esgotar o assunto, mas sim tornar mais habitual esse assunto que tem tudo para tomar um vulto com as descobertas de petróleos nos mares brasileiros e o crescimento dos portos brasileiros.

Desenvolvimento

Com o surgimento da necessidade de mais segurança nos portos e com a urgência em atender as normas do ISPS CODE, no primeiro semestre de 2004, que tem como objetivo melhorar os níveis de segurança dos portos e embarcações que atracam e desembarcam cargas nos diversos locais do mundo.

Surgiu à necessidade de criar um oficial de segurança portuário (Port Facilities Security Officer) PFSO que no Brasil ficou intitulado como Supervisor de Segurança Portuário (SSP), com a resolução que criava o SSP, algumas entidades de ensino começaram a buscar professores que conforme a norma as pessoas que eram reconhecidas PFSO perante aos EUA, estariam capacitados a ministrar o curso de ISPS CODE no Brasil, porém sem sucesso, pois o governo brasileiro, inicialmente deliberou o curso ministrado em Brasília – DF, somente com agentes, delegados e coronéis de diversos estados da federação com supervisão da polícia federal, por entender ser um assunto internacional e de relevância, para iniciar este curso que teve sua primeira turma em maio de 2004 sendo que a capacidade de formação era de aproximadamente 50 alunos para o Brasil inteiro, vemos que frente a essa quantidade ínfima de supervisor de segurança portuária (SSP) para um país que tem o maior porto da América Latina é muito pequeno esse contingente, inicialmente as pessoas que candidataram aos cursos em Brasília eram pessoas que não tinham perfil de segurança para atuar, algumas pessoas com cargo de gerência administrativa que provavelmente nunca iriam realizar tal tarefa, mas assim mesmo houve a aceitação destes no curso, atualmente, existem também pessoas que não trabalham mais na área portuária, então há necessidade de aumentar os critérios para formar os supervisores de segurança portuária, vale lembrar que a exigência do ISPS CODE tem que ter o SSP 24 horas por dia 7 dias na semana, hoje vemos pouca ou nenhuma atividade desse supervisor nos portos fazendo interface com os navios que aportam nos portos do Brasil, logicamente que existem alguns terminais e embarcações que exige esse cumprimento da norma, o que não ocorre na maioria dos terminais.

Precisamos entender que o ISPS CODE foi desenvolvido para proteção das embarcações e dos portos ao redor do mundo no Brasil foram

sendo criadas resoluções para ajuste do código, mas nessas resoluções, inexiste uma punição caso o terminal ou o porto não obtenha a DC (declaração de cumprimento), a única sanção é que este ficaria fora do comércio de produtos exportados para o EUA, correndo o risco de perder para a concorrência que está cada vez mais ávida de buscar novos clientes e em busca de um diferencial.

O porto de Santos recebeu sua DC somente em 15/12/2010, esta declaração certifica que o porto de Santos incluindo os terminais que fazem parte desse porto estão todos em de acordo com as normas do ISPS CODE, vale lembrar que cada terminal teve que elaborar o seu projeto de segurança sendo assessorado por várias empresas certificadas como RSO (Organização de Segurança Reconhecida), porém algumas RSO inicialmente certificadas eram empresas sem foco na segurança portuária, pois haveria necessidade de realizar análise de risco com foco em segurança patrimonial portuária, mas foi em alguns terminais imposto a necessidade de realizar tal análise, muito se viu em torno de custo e pouco se falou em qualidade, haja vista a qualidade das empresas, existiam diversas empresas com ramos de atividade completamente divergentes do objetivo do ISPS CODE, recentemente, foi reformulado o processo de cadastro das RSO no CONPORTOS, com visão de segurança portuária, na resolução nº44 da CONPORTOS de 17/02/2009, passou a ser exigido que as empresas que desejarem candidatar-se RSO necessitariam ter exclusivamente no seu objeto social do contrato a comercialização de bens destinados à utilização em projetos de segurança ou a prestação de serviços de segurança patrimonial, passou a ser exigido que a empresa mantenha no seu quadro de profissionais pessoas com conhecimento relevantes em segurança portuária, com capacidade de realizar análise de risco dos terminais e navios, fazendo a interface navio/porto, capacidade de identificar armas, dispositivos e artefatos perigosos ilícitos, entre outras imposições da resolução que é muito relevante para que a segurança portuária seja levada a sério realmente.

Dentro das normas do ISPS CODE foram criado três níveis de segurança, estes aprovados e analisados pela CONPORTOS (Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis) subordinado ao Ministério da Justiça, o nível 01 é o nível normal de segurança o que menos implementa medidas de controle e segurança, já o nível 03 necessita ter autorização do GSI (Gabinete de Segurança Institucional) que está ligado diretamente à presidência da república, neste caso há o envolvimento das forças armadas com o objetivo de impedir ação terrorista no porto ou embarcação. Todas as mudanças de nível necessitam de autorização da CONPORTOS e da CESPORTOS (Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis) este autoriza a mudança para o nível 02, sempre dentro do grau hierárquico que compete cada ato, vale lembrar que os terminais necessitam ter de pronto as medidas que passam de um nível para outro, pois essas mudanças ocorrem quando existe a exposição ao risco.

Foto - Rémi Kaupp

Conforme a revista Exame edição 973 de 11/08/2010, os EUA baixou uma medida em 2007 a fim de coibir o terrorismo nas cargas que adentrem nos portos americanos, medida esta que determina que todos os containeres passem por scanner no país de origem, ocorre que a quantidade de scanners que existe no Brasil para que seja verificado o interior dos containeres é insuficiente e a compra dos mesmos demora em torno de 18 meses, então vemos que poderemos ter problemas no ano de 2012 com a exportação para os EUA. O texto comenta que o maior prejudicado poderá ser o estado da Paraíba que exporta em torno de 52% das cargas exportadas para o EUA e neste não existe nenhum scanner.

No nosso Brasil ainda existe certo descaso com alguns dos cargos de segurança patrimonial, onde existem sempre cortes nessa área quando há necessidade de redução de gastos, porém não ocorre o pensamento da alta gestão de que não existem os sinistros em razão da existência de pessoas focadas nesses pontos, então podemos entender não como gasto, mas sim como investimento na área, logicamente que existem profissionais de segurança que não pensam da mesma forma. O perfil do gestor de segurança está mudando, hoje existem vários curso focados nesse nicho de mercado, que vão desde curso técnicos MBS (Master Business Security), cursos tecnólogos de gestão de segurança e MBA gestão de risco e segurança empresarial, certamente surgirão outras.

Conclusão

Ainda existe muito terreno a percorrer para conscientização de que a segurança nos terminais e embarcações é muito importante para a preservação da paz e a redução de exposição dos terminais e embarcações ao terrorismo e conseqüentemente estar aberto para alavancar divisas financeiras junto ao mercado dos EUA. Sabemos que nosso Brasil não levou a sério a implementação do ISPS CODE, uma vez que o maior porto da América Latina teve a sua Declaração de Cumprimento somente depois demais de seis anos de a medida ser assinada pelos países membros, onde a data limite para adequação do ISPS CODE foi julho de 2004, sem falar na necessidade urgente de adquirir os scanners até 2012 para monitorar os todas as cargas que irão para o EUA que provavelmente não haverá tempo para cumprir tal medida poderemos ter caos nas exportações, será necessário que o governo americano abra exceções na medida, adote o "jeitinho brasileiro" ou então teremos grandes problemas.

Referencias

Revista Exame, edição 973 de 11/08/2010, nº 14, ano 44, pag. 18, matéria comércio exterior que fala "Quem precisa do mercado americano?"

Fraud Risk Assessment

A fraude hoje nas empresas é um tema de preocupação estratégica, pois afeta de forma direta a competitividade e a imagem. As últimas pesquisas realizadas nos Estados Unidos, pelo ACFE, comprovou um aumento de 65% em relação ao ano de 2002.

Acreditamos, embora haja esta preocupação estratégica, que ainda exista muito o que fazer em termos de prevenção.

A Brasiliano & Associados avalia os riscos de fraudes nos processos das empresas e realiza auditoria investigativa. Oferecemos um trabalho independente, com uma visão prospectiva, utilizando ferramentas de tecnologia da informação voltados à prevenção, detecção e investigação.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Investigação de Fraude
- Gestão de Risco de Fraude – Mapeamento, Avaliação e Respostas ao Risco de Fraude
- Tecnologia Forense
- Verificação de Antecedentes – Background Checks Investigation
- Compliance em antilavagem de dinheiro
- Estruturação e Operacionalização de Canal de Comunicação – Denúncia
- Serviços de Ética Comercial
- Serviços de FCPA – Programas de Prevenção, Monitoramento e Controles Internos – Corrupção e Antisuborno

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

Forense Digital: Produzindo Provas Legais

Bianca Padovani - Advogada cursando MBA em Gestão de Riscos, Leandro de Jesus - Auditor em gestão de riscos cursando MBA em Gestão de Riscos e Rodrigo Segura da Silva - Analista de Segurança cursando MBA em Gestão de Riscos

Resumo

Com a evolução tecnológica e o surgimento da internet na atual era da informação surgiram muitas facilidades no dia-a-dia das pessoas como acessar sua conta do banco sem precisar sair de casa ou do trabalho fazer compras sem enfrentar um shopping lotado e outras. Essas facilidades também tornaram possíveis alguns tipos de crimes eletrônicos o que vem obrigando as agências legais e as empresas a se prepararem para investigar casos que envolvam incidentes digitas contudo muitas vezes o despreparo profissional e a má utilização das ferramentas na elucidação dos incidentes geram provas eletrônicas que podem ter seu valor jurídico contestado tornado assim todo trabalho de investigação nulo no artigo apresentamos algumas técnicas de investigação que podem fazer a diferença na comprovação de um ilícito seguindo boas práticas de análise e investigação digital que não comprometam as evidências coletadas.

Palavras-Chave: Forense; Digital; Provas; Eletrônicas; Investigação

Abstract

With technological progress and the emergence of the Internet in today's information age there were many facilities in day-to-day life of people accessing your bank account without leaving your home or work shop without facing a crowded mall and other facilities but these also made possible certain

types of electronic crime that is forcing the law enforcement agencies and businesses to prepare for investigating cases involving incidents Digital nevertheless often the lack of professional training and misuse of the tools in the elucidation of the incidents generate electronic evidence that may have their disputed legal status become so all research work in this paper we present some null investigative techniques that can make a difference in the proof of an illicit, following best practices research and analysis without compromising the digital evidenceected.

Keywords: Forensic; Digital, Proof, Electronic; Research.

Introdução

A Forense Digital é uma área de pesquisa relativamente nova são poucos os trabalhos sobre esse assunto no Brasil, entretanto é crescente a necessidade de desenvolvimento nesse sentido, haja vista que a utilização de computadores em atividades criminosas serem cada vez mais comum.

Por se tratar de uma necessidade muito recente, ainda não se conta com padrões internacionais para o tratamento desse tipo de evidência, dessa forma o valor jurídico de uma prova eletrônica manipulada sem padrões devidamente pré-estabelecidos poderia ser contestável.

Este trabalho é um estudo, que tem a finalidade de apresentar boas práticas de investigação digital para coletar, preservar e analisar evidências na reposta a incidentes de segurança que produzam provas que tenham valor legal incontestável.

Desenvolvimento

Também conhecida como Forense Computacional, pode ser definida como a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional.

A ocorrência mais comum no caso seria calúnia, difamação e injúria através do e-mail, roubo de informação confidências, remoção de arquivos, pedofilia, fraudes e tráfico de drogas via internet.

Objetivo da Forense Computacional:

Aplicar métodos científicos e sistemáticos, buscando extrair e analisar tipos de dados de diferentes dispositivos, para que essas informações passem a ser caracterizadas como evidências e, posteriormente, como provas legais de fato.

A forense computacional é empregada:

- Para fins legais (ex: Investigar casos de espionagem industrial);
- Em ações disciplinares internas (ex: uso indevido de recursos da instituição)

Para serem consideradas provas válidas, é muito importante que o perito realize o processo de investigação de maneira cuidadosa e sistemática. Deve preservar a integridade das evidências e gerar documentação detalhada.

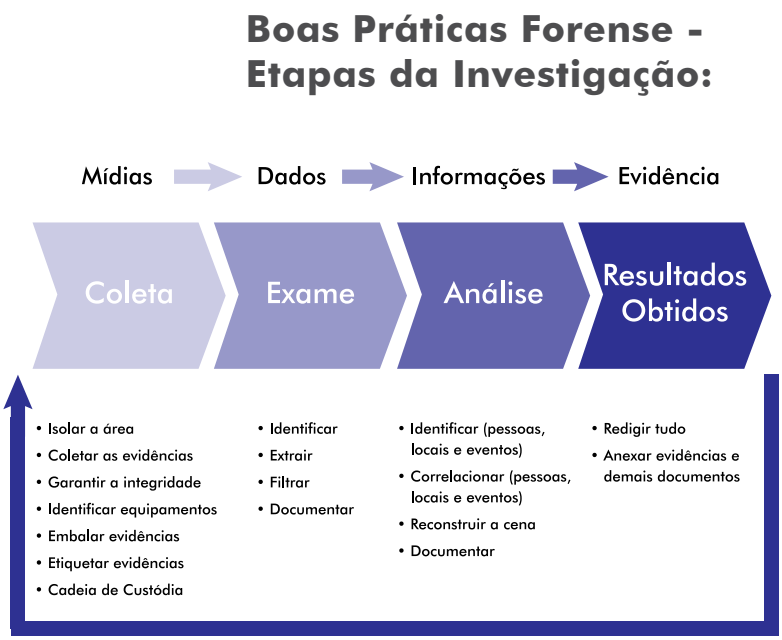


Figura 1 Fases de um processo de Investigação

Coleta de Dados:

Possíveis fontes de dados:

- Computadores Pessoais
- Dispositivos de Armazenamento em Rede:
- CDs, DVDs;
- Máquina Fotográfica, relógio com comunicação via USB, etc;

Os Dados também podem estar armazenados em locais fora dos domínios físicos da cena investigada. Ex Provedores de Internet, Servidores FTP (Fiel Transfer Protocol) e servidores Corporativos.

Nesses Casos, a coleta dos dados somente será possível mediante ordem judicial.

A cópia de dados envolve a utilização de ferramentas adequadas para duplicação dos dados, pois é de vital importância que seja garantida a preservação da integridade das evidências coletadas, pois caso isso não ocorra, as evidências poderão ser invalidadas como provas perante a justiça.

A garantia da integridade das evidências consiste na utilização de ferramentas que aplicam algum tipo de algorítmo hash.

Assim como os demais objetos apreendidos na cena do crime, os materiais de informática apreendidos deverão ser relacionados em um documento (Cadeia de Custodia).

Deve ser feito cópia lógica (Backup) do material a ser analisado, no mínimo duas cópias, uma para ser realizada coleta dos dados pertinentes a investigação e a outra copia deve ser guardada em um cofre, caso haja a necessidade de novas análises.

Durante a coleta de dados é muito importante manter a integridade dos atributos de tempo mtime (modification time), atime (acess time) e ctime (creation time) – MAC times.

Mactime: permite que a partir das informações contidas nos metadados dos arquivos e diretórios, uma visão cronológica dos acontecimentos seja mostrada.

Exame de Dados:

A finalidade desta etapa do processo é filtrar e extrair somente as informações relevantes à investigação.

Ex: O arquivo de Log do sistema de um servidor pode conter milhares de entradas, sendo que somente algumas delas podem interessar à investigação.

Após a restauração da cópia dos dados, o perito deve fazer uma avaliação dos dados encontrados:

- Arquivos que haviam sido removidos e foram recuperados;
- Arquivos Ocultos;
- Fragmentos de arquivos encontrados nas áreas não alocadas;

- Fragmentos de arquivos encontrados em setores alocados, porém não utilizados

Análise das Informações:

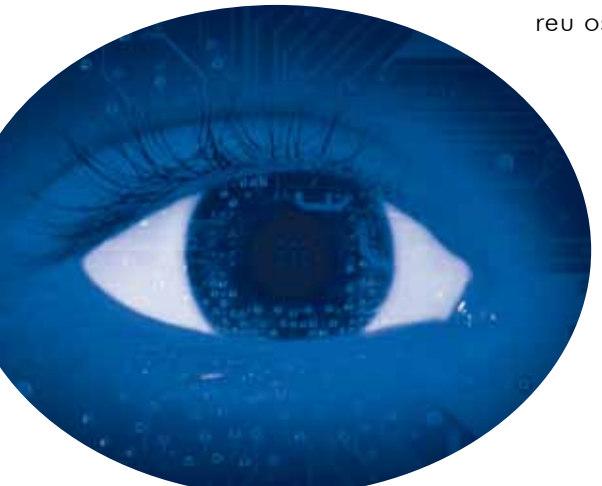
Após a extração dos dados considerados relevantes, o perito deve concentrar suas habilidades e conhecimentos na etapa de análise e interpretação das informações.

A finalidade desta análise é identificar pessoas, locais e eventos; determinar como esses elementos estão inter-relacionados. Normalmente e necessário correlacionar informações de várias fontes de dados.

Ex: Um indivíduo rouba a credencial de acesso e senha de um colega de trabalho, para acessar um sistema de gestão empresarial e utiliza essa credencial para faturar aparelhos celulares com desconto de 100% do valor do custo da Nota Fiscal, isso foi realizado em quantidade significativo, que gerou grande perda financeira para a empresa.

É possível identificar por meio de análise dos eventos registrados nos arquivos de log o endereço IP, data e hora de onde foi originada a transação.

Após a identificação do IP, é possível saber onde está localizada a máquina e correlacionar com os arquivos do banco de dados CFTV, as imagens da data e horário que foi realizada a transação, para identificar quem foi o indivíduo que estava utilizando a máquina no momento que ocorreu os eventos de fraude.



Resultados:

A interpretação dos resultados obtidos é a etapa final conclusiva da investigação.

O perito elabora um laudo pericial que deve ser escrito de forma clara e concisa, listando todas as evidências localizadas e analisadas.

O Laudo deve apresentar uma conclusão imparcial e final a respeito da investigação, para que o laudo torne-se um documento de fácil interpretação, é indicado que o mesmo seja organizado em seções:

- Finalidade da Investigação
- Autor do Laudo
- Resumo do incidente
- Relação de evidências analisadas e seus detalhes
- Conclusão
- Anexos
- Glossário (ou rodapés)
- Metodologia
- Técnicas
- Softwares e Equipamento empregados

Privacidade

Ao se fazer uma análise forense em uma máquina, sobretudo se ela atua como servidor de serviços, tais como e-mail ou arquivos deve-se tomar uma série de cuidados a fim de se evitar a invasão da privacidade dos usuários do sistema.

O problema da violação de privacidade muitas vezes pode ser contornado através da instituição de uma política de segurança clara e de conhecimento de todos os usuários, que contemple a possibilidade de vistoria em arquivos, e-mails e outros dados pessoais. Tal possibilidade deve ser seguida pela identificação de quem teria o poder para vasculhar os arquivos alheios, das

O surgimento de legislações e padrões a serem aplicados (Brasil), referente a forense Digital tornariam menor a chance de laudos serem inutilizados por falta de experiência dos peritos, pois a qualidade técnica da análise forense é muito importante para comprovação dos fatos denunciados.

circunstâncias em que essa medida pode ser tomada e de como o dono dos arquivos será notificado.

Análise de dados e sistemas deve ocorrer somente com autorização dos responsáveis ou ordem judicial.

Deve-se restringir a área da busca para não violar a privacidade de inocentes.

Aspectos Legais

No Brasil não existem normas específicas que regem a forense computacional, contudo existem normas gerais que abrangem todos os tipos de perícia (ditadas no Código de Processo Penal), podendo ser adotadas no âmbito computacional, salvo algumas peculiaridades. No caso de uma pericia criminal existe a figura de um Perito Oficial (dois para cada exame), onde seu trabalho deve servir para todas as partes interessadas (Polícia, Justiça, Ministério Público, Advogados, etc.).

A responsabilidade do Perito no exercício da sua função deve ser dividida em duas partes distintas: aquele do ponto de vista legal, onde lhe são exigidas algumas formalidades e parâmetros para a sua atuação como perito e as de ordem técnica, necessárias para desenvolver satisfatoriamente os exames técnico-científicos que lhe são inerentes[1]

O Perito deve seguir a risca as normas contidas no Código de Processo Penal, dentre elas pode-se destacar duas para exemplificar a sua possível abordagem computacional:

- Art. 170. Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.
- Art. 171. Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.

É de vital importância que se documente quais as ferramentas de software utilizadas para se fazer a análise, bem como a possível identificação de uma linha de tempo, que pode vir a ser conseguida através da análise dos MAC times.

Paralelos assim podem ser feitos a fim de se garantir o valor judicial de uma prova eletrônica enquanto não se tem uma padronização das metodologias de análise forense.

1 http://www.apcf.org.br

Conclusão

O surgimento de legislações e padrões a serem aplicados (Brasil), referente a forense Digital tornariam menor a chance de laudos serem inutilizados por falta de experiência dos peritos, pois a qualidade técnica da análise forense é muito importante para comprovação dos fatos denunciados.

A manipulação indevida das evidências em qualquer uma das etapas da investigação pode comprometer todo trabalho, pois dará margem para dúvidas na arbitragem, o que certamente tornara a prova contestável.

Enquanto não há legislação específica para perícia forense no Brasil, o emprego das melhores práticas de análise forense será determinante na conclusão do caso.

Supply Chain Risk Management - SCRM

A gestão de riscos da cadeia logística – Supply Chain Risk Management (SCRM) integra a organização, clientes, fornecedores e seu ambiente empresarial, reduzindo a dependência e promovendo a sinergia. Desta forma o gerenciamento contínuo dos riscos na cadeia logística passa a ser fonte de vantagem competitiva para todos neste processo.

Os riscos na cadeia logística podem afetar uns ou vários dos processos operacionais, podendo influenciar negativamente os objetivos de negócio. A gestão de riscos da cadeia logística é estruturado e sinérgico, aperfeiçoando a estratégia, os processos, os recursos humanos e a tecnologia. O foco é controlar, monitorar e avaliar o risco da cadeia logística visando garantir a continuidade o processo Supply Chain e aumentar sua resilência.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Implantação do Processo de Gestão de Riscos, com base na ISO 28000, 28002 e 31000;
- Elaboração no todo ou em partes do processo de Identificação, Análise e Avaliação e Tratamento dos Riscos na Cadeia Logística, com base na ISO 28000, 28002 e 31000;
- Elaboração e Implantação de Política de Gestão Riscos e da Gestão da Segurança para a Cadeia Logística, seguindo os preceitos da ISO 28000, 28002 e 31000;
- Elaboração e Implantação de Manuais de Contingência e Continuidade das Operações, seguindo os preceitos da ABNT NBR 15999, ISO 28000, 28002 e 31000;
- Elaboração de Processo de Comunicação e Consulta, incluindo as técnicas e ferramentas de sensibilização e conscientização para o público interno e externo;
- Preparação para a Certificação da ISO 28000.

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

Ana Paula Deodato

Falta de um plano de emergência é uma das principais causas das catástrofes naturais no Rio de Janeiro

O especialista em Gestão de Riscos Antonio Celso Ribeiro Brasiliano foi convidado pela Globo News, canal brasileiro de notícias, no dia 18 de janeiro de 2010, para falar sobre a catástrofe natural que aconteceu na Região Serrana do Rio de Janeiro em janeiro deste ano.

Brasiliano abordou quais foram os principais fatores que levou a falta de articulação e planejamento de contingência, como a falta de prevenção sem um plano bem estruturado e a falta da resposta de emergência, onde não houve estrutura, e nem processo pensado ou planejado anteriormente. A falta de comunicação e a falta de trabalho integrado possuem com causa processo de contingência entre órgãos como: Marinha, Exército e Defesa Civil, foram questões importantes para dar uma resposta mais eficiente nesta tragédia.

O governo Federal juntamente com a Desesa Civil devem que procurar investir em um plano de emergência bem estruturado para diminuírem as chances de o desastre vir acontecer novamente, elaborar uma boa analise de risco, encontrar as fragilidades, criar os cenários de riscos, ter recursos compatíveis com o tipo de cenário elaborado no plano de emergência, ter uma boa simulação e treinamento junto com uma boa comunicação, são essenciais para que isso não se ocorra novamente.

Ana Paula Deodato

Palestra Segurança na Cadeia Logística: Supply Chain Risk Management – SCRM ISO 28000

A Brasiliano & Associados, realizou no dia 20 de dezembro de 2010, na Faculdade FAPI/FESP a Palestra, Segurança na Cadeia Logística: Supply Chain Risk Management – SCRM - ISO 28000.

O evento foi ministrado pelo especialista Antonio Celso Ribeiro Brasiliano, Diretor Executivo da Brasiliano & Associados, abordando os processos e framework das normas ISO 28000 e ISO 31000, as integrações e interfaces, bem como suas especificações.

A palestra contou com algumas empresas participantes, tais como: Telefônica, Porto Seguro, Itaú Seguros, DHL, Tracker do Brasil e GRTRANSSAT.

Ana Paula Deodato

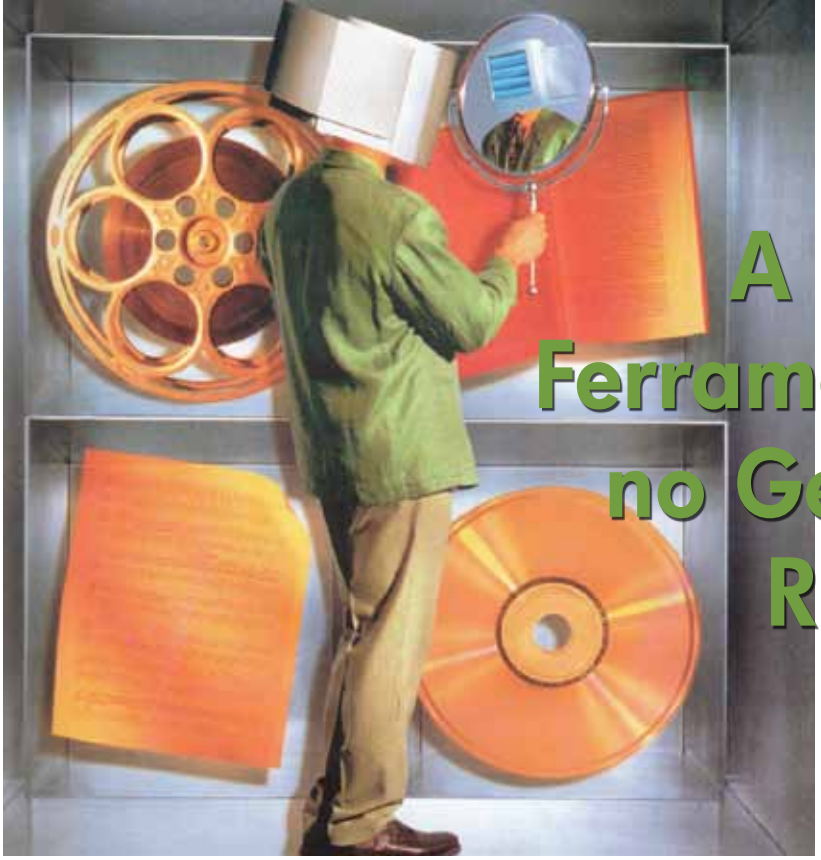
Sicurezza sorteia TV LCD entre seus visitantes

Sicurezza Editora realizou no dia 23 de dezembro, o sorteio de uma TV LCD 32 polegadas, para os clientes do site. Para participar da promoção os interessados deveriam gastar o valor mínimo de R$ 50,00 em compras de qualquer livro em estoque do site. A promoção ocorreu entre os dias 17 de outubro de 2010 a 22 de dezembro de 2010, entre os títulos publicados estão:

- As Formas do Crime
- Dicas de Segurança
- Guia Prático do Agente de Segurança
- Dicas e Macetes do Gestor de Segurança
- Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado
- Controle de Acesso: Conceitos, Tecnologias e Benefício
- A Questão da Segurança Privada

O Ganhador da promoção foi Antônio Albuquerque do Belém – Pará.

Parabéns ao ganhador!



A Importância das Ferramentas Sistêmicas no Gerenciamento de Risco Empresarial

Jéssica Mary dos Santos - , Marcos Elias

Resumo

As organizações em geral estão expostas a diversos tipos de riscos ambientais, legais, operacionais, financeiros e tecnológicos, entre outros, inclusive considerando que ausência do gerenciamento desses riscos causa muitos danos propiciando o seu declínio e pode levar até a sua extinção, sendo a proposta deste artigo é demonstrar as razões da necessidade da adoção de sistemas computadorizados para o bom gerenciamento de riscos empresariais, considerando que gerenciamento de riscos é uma atividade que vêm se desenvolvendo em ritmo cada vez mais acelerado, em especial, a partir dos anos 1990, impulsionado pelo aumento da complexidade das relações empresariais decorrentes do avanço do processo de globalização e pelo desenvolvimento de métodos ferramentas de gerenciamento e controle, sendo que contribuiu também de forma contundente, a maior conscientização das organizações, em decorrência de se haverem tornado públicos os problemas enfrentados por empresas consideradas em nível de excelência em razão da má gestão dos riscos a que estavam expostas, portanto, a diversidade dos tipos de riscos a que estão expostas as organizações e a multiplicidade de eventos e variáveis que lhes estão associadas, impõem a necessidade de alto nível de integração e análise das informações geradas pelo acompanhamento das atividades empresariais, tornando imperativa, a adoção de sistemas computadorizados para seu gerenciamento eficaz.

Palavras-chave: Riscos, Empresariais, Sistemas, Computadorizados, Gestão, Monitoramento.

Abstract

The organizations in general are exposed to different types of environmental risks, lawful, operational, financial and technological, among others the absence of the management of these risks cause much damage providing the decline and can even lead to its extinction the aim of this paper is to demonstrate the reasons for the need to adopt computerized systems for the proper management of business risks, the risk management is an activity that have been developing at increasingly rapid pace, especially from the 1990s, driven by the increasing complexity of business relationships resulting from the advance of globalization and the development of management tools, methods and control and he also contributed

forcefully, the increased awareness of the organizations, due to they had made public the problems faced by companies considered at the level of excellence because of the mismanagement of the risks they were exposed, and t0he diversity of the types of risks they are exposed to the organizations and the multitude of events and variables associated with them, impose the need for high level of integration and analysis of information generated by the monitoring of business activities, making it mandatory, adoption of computerized systems for their effective management.

Key Words: Risk, Business, Systems, Computerized, Management, Monitoring.

Introdução

As organizações têm seus objetivos definidos pela sua missão e visão, a partir dos quais, estabelecem processos para viabilizar a maximização dos resultados no seu cumprimento.

A ocorrência de fatores adversos são os riscos, os quais, materializando-se interna ou externamente a elas podem provocar, desde pequenos inconvenientes, até mesmo a sua extinção. A busca dos resultados desejados passa necessariamente pela administração eficaz desses eventos impeditivos, minimizando-lhes os impactos e pelo aproveitamento das oportunidades que o dinamismo do ambiente dos negócios oferece.

Disso resulta evidente, a necessidade de focar o gerenciamento de suas atividades, levando em conta a probabilidade da ocorrência desses fatores desfavoráveis, o impacto que seria gerado pela sua ocorrência e a análise perene do ambiente social, econômico, legal, político e mercadológico etc, em que está inserida, pois gerenciar riscos significa gerenciar a possibilidade de perdas ou redução de lucros, bem como a mensuração dos níveis de controle para mitigar os riscos da organização (Zonatto & Beuren 2010)

Esse gerenciamento permite que o gestor consiga, internamente, avaliar até que ponto as ações tomadas estão alinhadas com os objetivos traçados e, externamente, a análise situacional do momento e as tendências de evolução do ambiente, permitindo a tomada de medidas preventivas ou corretivas para evitar adversidades.

Desenvolvimento

Entre os diversos modelos de gerenciamento de riscos e controle interno disponíveis, destaca-se aquele elaborado pelo Comitê das Organizações Patrocinadoras – COSO – ERM (*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*) ou COSO II. Esse modelo é recomendado às empresas dos Estados Unidos, pela Lei *Sarbanes–Oxley* de 2002 que entre outras coisas, obriga e regulamenta a utilização de padrões éticos na elaboração das demonstrações financeiras aos investidores daquelas empresas, bem como das empresas brasileiras que têm seus ADRs (*American Depositary Receipt*) nas bolsas de valores daquele país.

O COSO II preceitua a observação de uma série de eventos que devem ser cumpridos para a gestão de riscos nas organizações, estabelecendo um ambiente de controle alinhado com os seus objetivos, sem, no entanto, tipificar os riscos a que ela está sujeita.

Para o COSO II, (2004, p. 16) "o risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos da empresa". A ocorrência de algum evento que afetará negativamente o cumprimento dos objetivos da organização.

Segundo a metodologia COSO, o gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados (Brasiliano, 2009, p 15), a saber: O ambiente interno, que é a expressão da cultura da empresa, fornece a base, a filosofia de gerenciamento de risco, a integridade, valores éticos etc. A fixação dos objetivos, que devem estar alinhados com a missão, a visão e com o apetite a riscos da organização, permitem a implementação de processos que suportem o gerenciamento dos riscos. A identificação de eventos internos ou externos que são classificados em riscos ou oportunidades, sendo, os riscos gerenciados e as oportunidades canalizadas para os processos de estabelecimento de estratégias ou de seus objetivos. A avaliação de riscos que deve considerar a probabilidade de ocorrência e o impacto, para determinar a forma pela qual serão gerenciados. A resposta a risco para a qual, em decorrência da avaliação e do apetite a riscos da organização, a administração escolhe a resposta mais compatível a cada tipo de risco, desenvolvendo medidas para evitar, mitigar, ou aceita-los. As atividades de controle que desenvolvem os processos e políticas para assegurar o eficaz cumprimento das respostas a riscos. As informações e comunicações que tratam da eficácia e tempestividade na divulgação seletiva das informações relevantes às partes interessadas, os *stakeholders* e, finalmente, o monitoramento que fará o acompanhamento permanente a nível gerencial e de auditorias interna e independente da integridade da gestão de riscos.

O gerenciamento de riscos não visa somente a prevenção e a gestão dos fatores adversos, mas também a identificação de oportunidades, muitas vezes invisíveis ao mercado, trazendo vantagens competitivas para a empresa.

Segundo Laudelino (2008 p. 43) "o gerenciamento de riscos por meio de uma análise eficiente de oportunidades de negócios permite que a empresa aproveite oportunidades de mercado que as outras empresas não podem aproveitar"

A definição a seguir reflete certos conceitos fundamentais. O gerenciamento de riscos corporativos é um processo contínuo e que flui pela organização, conduzido por seus próprios profissionais. É aplicado à definição das estratégias, em toda a organização, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta. Deve ser formulado de modo que identifique eventos em potencial, cuja ocorrência poderá afetá-la, e que administre os riscos de acordo com o seu apetite a risco, seja capaz de propiciar garantia razoável para a diretoria executiva e para o conselho de administração, e orientado à realização de

objetivos em uma ou mais categorias distintas, mas dependentes.

Conhecer e avaliar os riscos deixou de ser uma necessidade técnica para se transformar numa questão estratégica para as organizações, em função das exigências do mercado, governo, agências reguladoras e clientes.

Atualmente as organizações vêm atuando de forma mais precisa e preventiva no gerenciamento de riscos e, por isso, cresceu no mercado, a procura de ferramentas sistêmicas que ajudam na gestão de riscos.

Essas ferramentas permitem visualização dos riscos de diferentes formas, tais como: ativos, perímetros, componentes de negócio, ameaças, dentre outras. Contêm interface de uso simples e intuitivas, relatórios técnicos e executivos, controles de acesso, auditoria e proteção das bases de dados com criptografia, respostas de *checklists* e monitoramento (*followup*) por meio de indicadores.

Com o avanço da globalização e a disponibilidade de novas e avançadas tecnologias de gestão, a utilização de ferramentas sistêmicas para o gerenciamento de riscos tornou-se imprescindível. O que antigamente era um modelo de negócios, hoje é parte do processo do gerenciamento estratégico da maioria das organizações.

No entanto deve-se atentar ao fato de que não basta utilizar somente ferramentas computadorizadas para a gestão de riscos. Atualmente, a disponibilidade de softwares para gerenciamento de riscos se ampliou, tornando ainda mais necessário que a alta administração da empresa consulte seus profissionais de TI e de gerenciamento de riscos, para avaliar se a ferramenta oferecida pode ou não, ser aplicada com eficácia à estrutura da organização e se possui mecanismos de configuração e controles dinâmicos que mitiguem os riscos da própria ferramenta.

"o gerenciamento de riscos por meio de uma análise eficiente de oportunidades de negócios permite que a empresa aproveite oportunidades de mercado que as outras empresas não podem aproveitar"

Os sistemas computadorizados para gestão de riscos conquistaram seu espaço no mercado não somente pela redução no tamanho do arquivo físico dos mapeamentos dos processos, pela agilidade na atualização dos dados, pela facilidade e acesso a trabalhos, precisão e eficácia nos indicadores de resultados, geração automatizada de relatórios e gráficos e otimização da produtividade da equipe. Fizeram-no também na preservação da memória que permite a identificação e histórico das inclusões, exclusões e alterações realizadas no sistema.

Como toda ferramenta, os softwares de gestão de riscos também possuem um lado frágil. Se, por um lado, ajudam a detectar novas oportunidades e criar vantagens competitivas, por outro, se não forem adequadamente estruturados, podem trazer ameaças, tais como: perda das informações, insuficiência na capacidade de armazenamento de dados x volume da organização, fragilidade no ambiente de configuração (controle de acessos), entre outros.

Por isso para uma implantação eficiente, eficaz e segura de software de gerenciamento de riscos é necessário que a alta administração avalie a capacidade (porte x custo benefício x objetivo estratégico) da organização e possua ferramenta de controles que mitiguem os riscos que possuem maior probabilidade e impacto de ocorrência na organização. Possuindo, por exemplo, estruturas para *back up* dos dados do software, armazenado em local distinto, acesso

restrito às configurações do software, trilha de auditoria para registros contendo o *login* e o *IP*[1] dos acessos, plano de contingência formalizado para o caso de *disaster recouver* e monitoração periódica dos acessos, dados e *back up* do software.

Referencial Teórico

A base que fundamentou a elaboração deste artigo, com relação à exposição das organizações a riscos corporativos e à sua gestão eficaz, está calcada principalmente na metodologia COSO e no Método Brasiliano Avançado de Gestão e Análise de Riscos Corporativos.

Com relação às ferramentas sistêmicas para o gerenciamento de riscos, dada a escassez de literatura técnica acadêmica a respeito, foram feitos estudos de mercado e participação em palestras com empresas que fornecem software de gerenciamento de riscos.

Metodologia

Esta pesquisa tem caráter descritivo e foi realizada por meio de análise documental, com a finalidade de evidenciar os aspectos consonantes à justificativa apresentada.

Conclusão

Ao apresentar, ainda que resumidamente, a multiplicidade de fatores intervenientes na gestão eficaz dos riscos corporativos, fica demonstrada a impossibilidade de levá-la ao sucesso sem o auxilio de uma adequada ferramenta de sistema de processamento de dados. Essa ferramenta deve revestir-se, no mínimo, das características essenciais apresentadas, para que consiga fornecer, com a agilidade e precisão necessárias, a integração de dados e informações, bem como, as análises contextuais e operacionais ao eficaz cumprimento de sua finalidade.

1 Internet Protocol

Referências

BRASILIANO, Antonio Celso Ribeiro. *Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado*. Sicurezza Gestão de Riscos Corporativos, Editora e Distribuidora Ltda. 1ª Edição, 2009

COSO – Comitee of Sponsoring Organizations of the Treadway Commission – *Gerenciamento de Riscos Corporativos* – Estrutura Integrada – Sumário Executivo. Disponível em: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf Acesso em 09.08.2010

FILHO, Emílio Herrero *Balanced Scorecard e a Gestão Estratégica* – Uma abordagem prática, ed Campus – 2005

LAUDELINO, Júlien Ariani de Souza. *Evidenciação de Riscos de Empresas que Captam Recursos no Mercado de Capitais Brasileiro* – Um Estudo do Setor de Energia Elétrica. 2008 183 f Dissertação (Mestrado em Ciências Contábeis) – Universidade Regional de Blumenau, Blumenau, 2008

PWC – PRICE WATERHOUSE E COOPERS. *A importância da gestão de riscos nos processos de auditoria*. 2002. Disponível em: http://www.ebah.com.br/a-importancia-da-gestao-de-riscos-nos-processos-de-auditoria-pdf-a18760.html Acesso em 08/08/2010

ZONATTO, Vinícius Costa da Silva e BEUREN, Ilse Maria. Categorias de Riscos Evidenciadas nos Relatórios da Administração de Empresas Brasileiras com ADRs – *RGBN – Revista Brasileira de Gestão de Negócios* – Vol. 12 – número 35 – Abril / Junho 2010

Business Continuity Management – BCM
Gestão da Continuidade de Negócios - GCN

Sua empresa está preparada para um evento de DESCONTINUIDADE??

A operacionalização de um GCN é um processo estruturado para:

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

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

No Brasil, através da ABNT, tem as normas ABNT NBR 15999 - 1 e 2, que descrevem o processo, estrutura e conteúdo de um sistema de Gestão de Continuidade de Negócio.
A empresa deve possuir resilência. A Brasiliano & Associados ajuda a sua empresa a manter o fôlego, mesmo em momentos críticos.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Mapeamento dos Processos Críticos, através de critérios personalizados para o tipo de negócio – BIA – Business Impact Analysis
- Estabelecimento de Critérios de Tempo de Resposta e Tempo de Recuperação
- Elaboração de Estratégias de Continuidade
- Elaboração de Procedimentos Operacionais
- Estrutura Organizacional da Continuidade e da Crise
- Programas de Comunicação de Crise
- Programas de Sensibilização
- Testes Operacionais e de Conformidade

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

Ler & Saber

Ana Paula Deodato

BREVE LANÇAMENTO - Gestão Estratégica do Sistema de Segurança Conceito, Teorias, Processos e Prática

Ao falar em Gestão Estratégia do Sistema de Segurança, o professor Nino Ricardo Meireles, apresenta em sua obra, temas para empresas especializadas na prestação de serviço de segurança privada como, teoria de sistemas denominando suas funções, teoria das falhas fazendo uma análise de como as falhas podem acontecer dentro de uma empresa e a teoria das restrições indicando seus princípios e suas melhorias.

O autor traz ao leitor uma explicação mais detalhada sobre os tais temas, deixando mais claro as informações que o Gestor de Segurança procura tanto para a prevenção de perdas dentro das organizações até a gestão estratégica nos processos de segurança empresarial, além de ser uma obra didática oferecendo uma ferramenta para quem busca a prevenção e estratégica, "O objetivo da estratégia é encontrar uma posição na qual a empresa seja capaz de melhor se defender contra as seguintes forças: clientes, fornecedores, entrantes em potencial, produtos substitutos e concorrentes." Afirma o autor.

O objetivo do autor é abordar assuntos didáticos de uma forma concreta para que o leitor aprenda a se adaptar com as mudanças de comportamentos competitivos que o mercado exige, com linguagens claras e objetivas.

Nino Ricardo Meireles é Engenheiro civil; Especialista em Consultoria e Gestão de Recursos

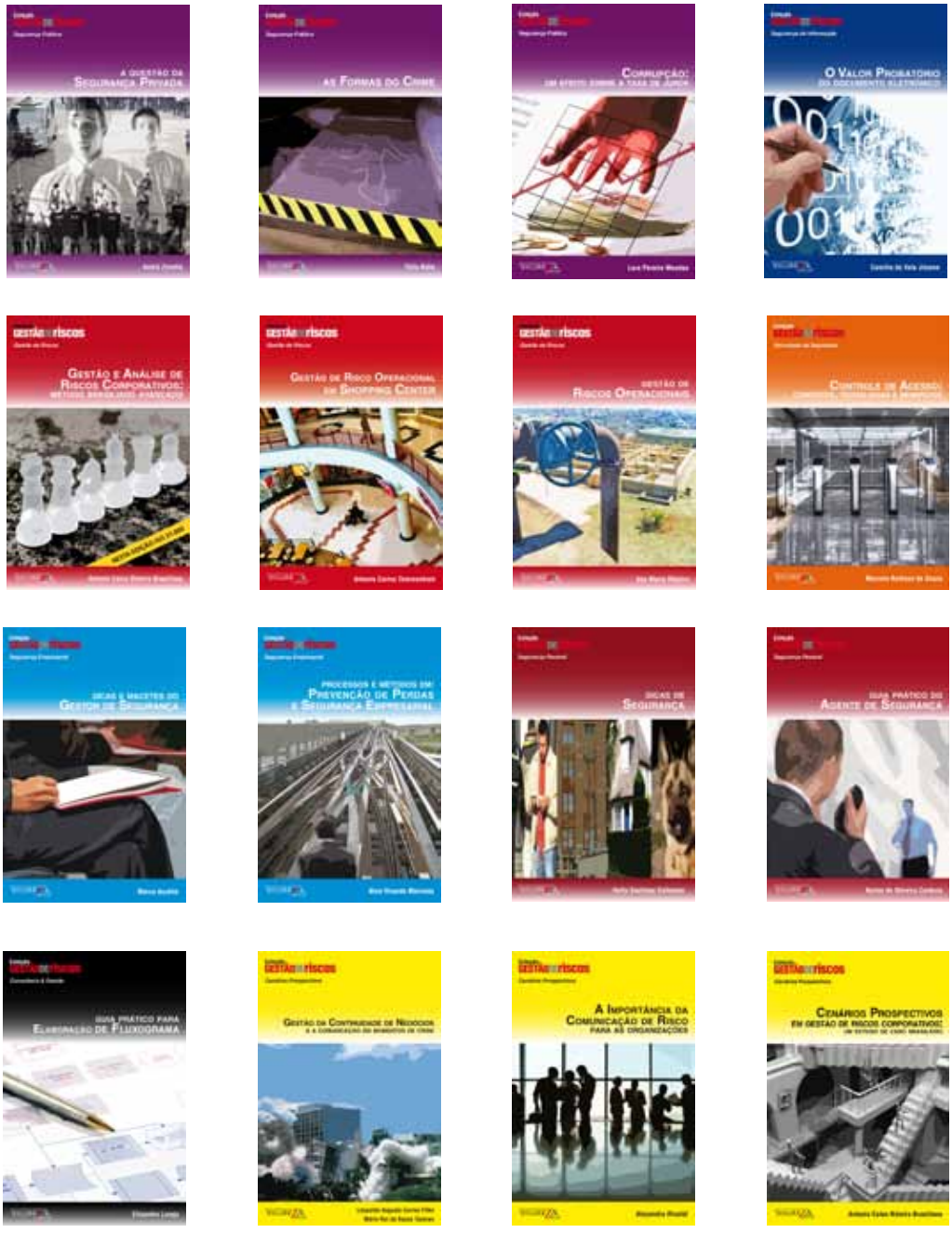
Humanos; Especialista em Gestão Estratégica de Negócios; Extensão em Administração da Segurança Empresarial; Extensão em Gestão de Riscos Corporativos; Coordenador e professor do Curso de Graduação Tecnológica em Gestão da Segurança Privada (Estácio, Centro Universitário da Bahia FIB); Coordenador e professor do MBA em Gestão

Estratégica da Segurança Corporativa (Estácio, Centro Universitário da Bahia FIB); Coordenador da especialização em Engenharia e Segurança do Trabalho (Estácio, Centro Universitário da Bahia FIB); Diretor estadual da Associação Brasileira dos Profissionais de Segurança (Abseg); Consultor, facilitador e pesquisador.

Ler & Saber

Editora Sicurezza, trazendo a informação!!

CONFIRA AS PUBLICAÇÕES



para comprar acesse: www.sicurezzaeditora.com.br

SICUREZZA editora

você sabe o que é Risco Social ?

PSSE projetos de sustentabiliade social empresarial

A missão da PSSE é contribuir para a sustentabilidade competitiva dos negócios dos nossos Clientes, por meio da análise dos impactos socioambientais de seus projetos e operações e implementação de medidas que mitiguem os riscos sociais, ambientais e de imagem corporativa.

A empresa oferece ao mercado empresarial brasileiro uma ferramenta importante na minimização de riscos sociais de empreendimentos, além de mostrar que ter a sede e as principais unidades sustentáveis é uma forma de grande visibilidade.

Seu objetivo é agregar valor à percepção de imagem corporativa de responsabilidade socioambiental, segurança integrada do empreendimento e identificação de medidas para inclusão social local.

A PSSE é uma Joint Venture entre a SustentaX e a Brasiliano & Associados.

PSSE
Projetos de Sustentabilidade Social Empresarial

SUSTENTAX

b&a
BRASILIANO & ASSOCIADOS

Informações: info@brasiliano.com.br - www.brasiliano.com.br - 11 5531 6171