

FUNDAÇÃO GETULIO VARGAS

ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS

MBA EM GESTÃO DE SEGURANÇA CORPORATIVA

ANÁLISE DE RISCOS NA ÁREA DE SEGURANÇA CORPORATIVA:

IDENTIFICAÇÃO E DESENVOLVIMENTO DOS FATORES

RELEVANTES EM TODAS AS ETAPAS DO PROCESSO

Cláudio Ferreira Caldas

Rio de Janeiro
2003

FUNDAÇÃO GETULIO VARGAS

ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS

MBA EM GESTÃO DE SEGURANÇA CORPORATIVA

ANÁLISE DE RISCOS NA ÁREA DE SEGURANÇA CORPORATIVA:

IDENTIFICAÇÃO E DESENVOLVIMENTO DOS FATORES

RELEVANTES EM TODAS AS ETAPAS DO PROCESSO

Cláudio Ferreira Caldas

**Monografia apresentada ao curso de pós
graduação em gestão de segurança
corporativa, como requisito para obtenção
do Certificado de Especialista.**

**Rio de Janeiro
2003**

SUMÁRIO	Páginas
1. INTRODUÇÃO	3
2. DESENVOLVIMENTO	5
2.1: <u>Diferenças Conceituais E Uniformização de Termos.</u>	5
2.2: <u>1ª Fase Do Processo de Análise de Riscos.</u>	10
Reconhecendo e Definindo os Ativos à Proteger	
2.3: <u>2ª Fase do Processo de Análise de Riscos.</u>	16
Identificação das Ameaças.	
2.4: <u>3ª Fase do Processo de Análise de Riscos.</u>	27
Reconhecendo as Vulnerabilidades.	
2.5: <u>4ª Fase do Processo de Análise de Riscos</u>	32
Identificação, Análise e Avaliação de Riscos.	
2.6: <u>5ª Fase do Processo de Análise de Riscos.</u>	45
A Importância da Gestão de Riscos nas Corporações	
3. CONCLUSÃO	52
4. ANEXOS	53
5. BIBLIOGRAFIA	74

1- INTRODUÇÃO

O RISCO E A IMPORTÂNCIA DE SEU GERENCIAMENTO

Desde os primórdios, observamos no comportamento humano a preocupação com a proteção dos bens ou “ coisa valiosa” . Com a percepção do que era importante para sua sobrevivência e manutenção da espécie, o homem primitivo, criou instintivamente, os primeiros meios para proteção destes ativos contra os riscos da natureza, animais selvagens e até outros homens.

Naturalmente, como a evolução não beneficiou a todos da mesma forma, a diferença entre os homens aumentou ainda mais a necessidade de proteção dos bens, dentro da própria comunidade.

Mesmo nesta época, o descaso ao proteger esta “coisa valiosa”, podia significar perdas irreparáveis, como a própria vida.

Alguns séculos se passaram, e com o desenvolvimento da civilização, a sensação de insegurança aumentou, já que o homem percebeu que não só a vida, o alimento e a moradia precisavam ser preservadas. Novas ameaças entravam em cena, e novos ativos como informações, imagem, bens móveis e imóveis, cidades e até países precisariam também de uma atenção especial, aumentando ainda mais o seu estado de medo e ansiedade.

Naquele momento, era essencial que o homem reconhecesse que apenas reagir, não seria suficiente para evitar danos causados pela materialização das ameaças existentes. Medidas preventivas, deveriam ser o componente mais forte na proteção, que tem como o objetivo final a segurança.

Muitos anos se passaram até nossos dias, e naturalmente nosso catálogo de ameaças se tornou mais extenso. Cidades cada vez mais populosas, organizações criminosas economicamente poderosas, uma maior competitividade nos negócios, o avanço tecnológico nas comunicações, maior velocidade nos transportes e maiores níveis de poluição tornaram a percepção, avaliação e gerenciamento de riscos, vitais à continuidade e preservação da vida, dos negócios, do meio ambiente, enfim de todo o desenvolvimento no planeta.

2- DESENVOLVIMENTO

CAPÍTULO 01

DIFERENÇAS CONCEITUAIS E UNIFORMIZAÇÃO DE TERMOS

Toda profissão, ou mesmo área de atuação possui uma terminologia própria e definições específicas. Apresentarei agora, uma lista de termos mais utilizados na área de análise e gerenciamento de riscos, com o objetivo de tentar esclarecer as dúvidas que ainda existam, estabelecendo comparações e diferenças entre as escolas americana e espanhola.

No entanto, ao iniciarmos nosso trabalho, é preciso compreender que o sucesso nesta área dependerá do perfeito de entendimento destes conceitos fundamentais, que estarão sempre presentes durante todo o processo. É importante também ressaltar, o grande dinamismo dos riscos na atualidade exigindo do profissional de segurança atual, uma maior percepção do meio ambiente onde se processa a identificação, análise e avaliação de riscos e seu posterior gerenciamento, tornando este trabalho contínuo e flexível ao longo do tempo.

1º) Ativos / Assets / Biens

Definições:

Escola Americana

“Qualquer pessoa, equipamento, infra-estrutura, material, informação, ou atividade que tenha valor positivo para seu proprietário. Também tem que ter valor para seus adversários.

A natureza e a magnitude destes valores podem se diferenciar drasticamente”
(Roper,1999, p.13)

“Identificamos os ativos de uma empresa, respondendo a pergunta: “ O que um empresa tem, opera, controla, usa , tem a custódia sobre, tem a responsabilidade sobre, compra, vende, produz, projeta, manufatura, testa, analisa ou mantém?

(Broder, 1999, p.7)

Escola Espanhola

“É toda pessoa, bem ou meio ambiente suscetível de sofrer danos ou perdas como consequência de ter sido submetido a um risco”. (Gómez- Merelo 1997, p.32)

“É toda pessoa ou coisa, que em determinadas circunstâncias, possui ou se atribui uma qualidade ou várias qualidades benéficas, em virtude da qual se torna um objeto de valor. É por tanto chamada de coisa valiosa ou qualidade benéfica”.
(Gómez – Merelo 1997, p.32)

2º) Ameaça / Threats / Amenazas

Definições:

Escola Americana

“Qualquer indicação, circunstância ou evento, com potencialidade de causar perdas ou danos a um ativo. Poderá ser definido também, como a intenção ou capacidade de um adversário empreender ações nocivas ou danosas aos interesses do proprietário destes ativos” (Roper 1999 , p.13)

Escola Espanhola

- “A ameaça é a causa potencial do dano. Difere do risco e do dano, que constituem parâmetros de valoração ou avaliação das ameaças.

(Equipe de Editorial - CPD 2000, p.112)

3º) Riscos / Risks / Riesgos

Definições:

Escola Americana

“A possibilidade de causar danos ou perdas a um ativo” (Roper 1999, p.13)

“A probabilidade de uma perda ocorrer no presente ou no futuro” (Broder 1999, p.1)

Escola Espanhola

“É todo agente ou situação que causa um dano ou perda de forma real ou potencial”. (Gómez – Merelo 1997, p.32)

4º) Vulnerabilidade / *Vulnerability*

Definições:

Escola Americana

“Qualquer debilidade que pode ser explorada por um adversário que possibilitará o acesso a um ativo”. (Roper 1999, p.14).

5º) Impacto / *Impact* / *Daño*

Definições:

Escola Americana

“O montante ou quantia, resultante do dano ou perda”. (Roper 1999, p. 13)

Escola Espanhola

“É toda variação real ou suposta, que um bem experimenta quando sofre uma diminuição de seu valor ou preço. Se caracteriza pelo seu agente causador, sua forma de manifestação e suas conseqüências negativas”. (Gómez – Merelo 2000, p.41).

6º) Avaliação de Riscos / Risk Assessment / Evaluación de Riesgos

Definições:

Escola Americana

“Processo de avaliar as ameaças e vulnerabilidades de um ativo, de modo a formalizar uma opinião sobre a probabilidade de ocorrência de um dano ou perda, e seu conseqüente impacto, que servirá como referencial para uma tomada de decisão positiva.”(Roper 1999, p.14)

Escola Espanhola

“É o processo pelo qual se faz uma valoração quantitativa e qualitativa dos fatores de risco, que incidem sobre uma determinada atividade. (Gómez – Merelo 2000, p. 39)”.

CAPÍTULO 02

1º FASE DO PROCESSO DE ANÁLISE DE RISCOS

RECONHECENDO E DEFININDO OS ATIVOS À PROTEGER

Nos anos que se passaram, o setor de segurança corporativa tinha o objetivo de proteger o patrimônio das empresas de uma forma total. O foco naquele momento era claramente o patrimônio físico da instituição, não havendo ainda o entendimento que a segurança, deveria dedicar-se a proteção dos ativos realmente importantes para a manutenção do negócio, tornando-se uma parceria, juntamente com as outras áreas estratégicas da empresa na busca de melhores índices de lucratividades e competitividade.

Segundo o relatório Pinkerton 2002, entre os principais desafios dos departamentos de segurança, está a redução dos orçamentos, alcançando este ano o 1º lugar, contra um 3º lugar nos anos de 2000 e 2001.

Isto demonstra claramente, que já nos dias de hoje teremos que selecionar de forma mais criteriosa os ativos à serem protegidos, já que será impossível pela redução dos orçamentos, a extensão desta proteção a todos eles.

Para isto, teríamos que definir quais seriam os de maior criticidade para empresa, para seus negócios e para manutenção de suas atividades.

As indagações que deveriam ser levados em consideração nesta seleção seriam:

1) Qual é a missão da empresa, seu diagnóstico estratégico e os elementos prescritivos de seu planejamento?

2) Quais os fatores críticos de sucesso da empresa?

3) Quais e em que proporções, estes ativos participam da atividade principal da empresa?

4) Quais as perdas decorrentes sobre estes ativos, caso aconteça algum evento indesejável?

5) Qual o impacto, provocado por estas perdas, no negócio?

É importante neste momento, ressaltar que os valores de um ativo podem não estar representados em valores de moeda corrente, e sim por vidas, interesses organizacionais, político e econômicos.

Segundo Carl Roper (1999, p.32) as condições associadas a estes valores seriam:

1) Exclusividade do ativo: Este ativo é encontrado apenas nesta empresa?

2) Reposição do ativo: Em quanto tempo e em que condições consigo repor este ativo?

3) Criação e recriação do ativo: O custo para a criação deste ativo é tão alto que seria impossível recriá-lo? (refere-se a pesquisa e projetos)

4) Impacto por danos ao ativo: Este ativo é essencial para a continuidade das operações da empresa, conclusão de projetos e implementação de novos programas?

Agora que já sabemos porque devemos selecionar criteriosamente nossos ativos, o que deveremos levar em consideração em nossa seleção, e os valores que estes devem ter para que possamos priorizá-los, será necessário, enumerá-los de forma abrangente, não focando nenhum tipo de negócio em especial.

A escola americana de segurança divide os ativos normalmente em 03 grandes grupos:

- a) **Pessoas**
- b) **Bens Tangíveis e Intangíveis**
- c) **Informação**

Carl Roper (1999, p.33), no entanto, detalha esta classificação considerando 05 grupos:

- a) **Pessoas**
- b) **Atividades e Operações**
- c) **Informação**
- d) **Instalação Física**
- e) **Equipamentos e Materiais**

Já a escola espanhola, difere um pouco da americana, apontando os ativos da seguinte forma:

- a) **Pessoas** – ressaltando como fator de relevância a saúde, integridade física, seus bens e patrimônio, sua intimidade, comunicações e integridade moral.

b) Bens e Patrimônio – ressaltando a importância das propriedades públicas, residências, hotéis, igrejas, centros de lazer, instalações militares, museus, indústrias, escolas etc...

c) Meio Ambiente – destacando a importância ao ar, a água, a terra, a fauna e flora.

Como podemos observar, é clara a diferença entre as duas escolas. A escola americana está focada mais na área de negócios e seus resultados, protegendo seus ativos de acordo com o impacto que as perdas poderiam ocasionar. Já os ensinamentos da escola espanhola de segurança, parecem ter um foco mais holístico, dando grande importância ao ser humano e ao meio ambiente.

Como próxima etapa de nosso trabalho, precisaremos definir as fontes que informarão quais os ativos essenciais para a nossa avaliação. Naturalmente, as pessoas mais indicadas são os usuários destes ativos, como por exemplo gerentes de departamentos, chefe de operações e dos departamentos de segurança. É muito importante a integração com os níveis gerenciais da empresa, assim como consultas a entidades de classe, sindicatos, fontes do governo, revistas, jornais, livros e sites na internet sobre empresas similares.

Desta forma, você poderá organizar questionários que permitirão obter um conhecimento maior sobre a empresa analisada, e os ativos que representam verdadeiro valor para o negócio. Mensurar este valor, será essencial para que

possamos assumir uma posição justificada perante a diretoria da empresa, para justificar no futuro, nossos investimentos em proteção.

Para nos auxiliar nesta missão, James Broder (1999, p.39), nos sugere uma matriz para classificarmos os níveis de impacto sobre os ativos e seus efeitos.

1	2	3	4	5	6	Nível de Impacto
Perda ou lesões graves de vidas humanas	Perda de Informação Secreta	Perda de Informação Confidencial	Perda de Informação sensível não classificada	Prejuízos ou paralisação nas operações, programas ou projetos	Danos ou perdas de bens de valor elevado	
Sim	Sim / Não	Sim / Não	Sim / Não	Sim / Não	Sim / Não	Crítico / Alto
Não	Sim	Sim / Não	Sim / Não	Sim / Não	Sim / Não	Alto
Não	Sim / não	Sim	Sim / Não	Sim	Sim / Não	Alto
Não	Sim / Não	Sim / Não	Sim	Sim	Sim / Não	Alto
Não	Não	Não	Não	Sim / Não	Sim	Médio
Não	Não	Não	Não	Sim	Sim / Não	Médio
Não	Não	Não	Não	Não	Não	Baixo

Fonte: Risk Management for Security Professionals - 1999

CRITÉRIOS PARA TOMADA DE DECISÃO

- **Nível Crítico** - Caso o ativo em questão sofra algum evento indesejável, as conseqüências serão perdas ou lesões graves à vida humana.
- **Nível Alto** - Caso o ativo em questão, sofre algum evento indesejável, as conseqüências serão a perda de informações confidenciais e secretas, com prejuízo das operações por um período determinado de tempo.
- **Nível Médio** – Caso o ativo em questão, sofra algum evento indesejável, as conseqüências serão a perda de informação confidencial e sensível ou danos à bens de valores elevados. Poderá haver prejuízos nas operações por um período determinado de tempo.
- **Nível Baixo** – É constatado pequeno ou nenhum impacto sobre vidas humanas, e tampouco na continuidade das operações.

Fonte: Risk Management for Security Professionals - 1999

CAPÍTULO 03

2ª FASE DO PROCESSO DE ANÁLISE DE RISCOS

IDENTIFICAÇÃO DAS AMEAÇAS

Dando prosseguimento ao nosso estudo, a segunda fase do processo de análise de riscos será a classificação das ameaças em diversos grupos, estabelecendo uma ligação com o grupo de ativos selecionados para proteção. O grande desafio para o profissional de segurança nesta etapa, será identificar as novas ameaças que surgem diariamente no cenário mundial, cada dia mais incerto; analisá-las e valorá-las de modo que consiga minimizar os danos causados por sua eventual materialização; e por fim conscientizar a alta gestão das empresas sobre a necessidade de investimentos em sua área de atuação.

Toda esta percepção no entanto, está intimamente ligada com a formação deste novo profissional, que não deverá ter obrigatoriamente uma extensa experiência nas áreas militar ou policial, e sim uma forte orientação corporativa, já que existe uma grande necessidade de se falar uma “mesma língua” com os altos executivos das empresas.

Infelizmente esta visão não é compartilhada por todos. Em um artigo publicado na revista *Security Management* de janeiro de 2003, intitulado *The New Centurions*, algumas empresas relatam, que após o atentado do dia 11 de setembro, tem dado preferência a profissionais com experiência nas áreas de informações e

investigações. No mesmo artigo George Campbell, presidente da *International Security Management Association (Isma)*, enfatiza que muitas empresas procuram, através desta instituição, profissionais com experiência policial ou militar, e não *MBA's*.

Campbell, no entanto, afirma que o mais importante não é o tipo de especialização, e sim que eles representem o que há de melhor na área.

Na verdade, a contratação deste profissional estará ligada intimamente a estrutura da empresa, definida pelo seu planejamento e políticas empresariais. Será muito importante estar bem definido qual a missão da empresa, seus objetivos, desafios e valores, suas políticas e estratégias e sua visão para o futuro. A formalização de tudo isto, permitirá ao profissional de segurança empenhado em realizar uma gestão estratégica de riscos, a ter uma percepção específica do ambiente direto e indireto à empresa no momento de identificar informações pertinentes ao seu trabalho. Desta capacidade de selecionar, coletar e analisar informações, dependerá sua maior ou menor percepção com relação às ameaças existentes.

Conforme vimos no segundo capítulo deste relatório, de acordo com as escolas americana e espanhola de segurança, ameaça é “qualquer indicação, circunstância ou evento com potencialidade de causar perda ou danos a um ativo”.

Na definição acima, identificamos que a ameaça não é somente um evento isolado como por exemplo roubo, sabotagem, explosão ou uma inundação. Poderá também ser definida como uma circunstância ou tendência.

A consultoria de segurança Brasileiro e Associados, por meio de sua ferramenta informatizada *Risk Report*, número 00 de 10 de outubro de 2002, analisando informações coletadas no meio ambiente, publicou uma relação de tendências para a área de segurança empresarial.

Muitas delas deverão ser encaradas como ameaças às empresas brasileiras pois podem afetar direta ou indiretamente seus ativos importantes. São elas:

Tendências Sócio – Demográficas e Tecnológicas

- Manutenção, sem solução, de questões sociais, como a má distribuição de renda, valorização do consumo e exclusão social;
- Permanência de grande parte da população brasileira sem acesso a educação secundária;
- Permanência dos atuais níveis de pobreza;
- Continuação das desigualdades sociais de consumo.

Tendências na Área de Segurança Pública

- Dificuldades na unificação e articulação entre as polícias;
- Continuação do baixo efetivo e da ineficiência das polícias;
- Falta de um sistema único de inteligência policial;
- Falta de integração entre a segurança pública e privada;

- Manutenção da ineficiência do sistema judiciário.

Tendências do Crime

- Aumento do número de homicídios, principalmente em função do crescimento da violência urbana;
- Crescimento do seqüestro relâmpago cometido por quadrilheiros ou amadores, cujo objetivo é roubar pequenas quantias (caixa eletrônico, compras em lojas etc.);
- Crescimento da terceirização do crime, como por exemplo nos casos de seqüestro, com a sub empreitada dos cativeiros;
- Aumento do roubo de lojas, supermercados e bancos;
- Crescimento da sensação de impunidade;
- Aumento dos crimes cibernéticos (ataques à redes de computadores e bancos de dados dentro e fora da empresa);
- Aumento das fraudes principalmente por meio eletrônico, cometidas por empregados, ou com o apoio de empregados da própria corporação, em função da insatisfação ou da falta de compromisso existente entre eles e a empresa;
- Crescimento da espionagem industrial em função do aumento da competição e redução das margens de lucro.

Tendências de Comportamento da População Brasileira

- Menor confiança da sociedade nas organizações policiais e no sistema de justiça criminal;
- Aumento das reclamações de invasão de privacidade nas empresas e órgãos governamentais, pela utilização de tecnologia de circuito fechado de televisão;

Tendências de Comportamentos das Empresas no Brasil

- Aumento da vulnerabilidade dos executivos das empresas, em função do crescimento da violência urbana e do crime organizado;
- Aumento do custo das empresas com seus funcionários em função da violência urbana, que provoca ausência ao trabalho, perda por morte, menor produtividade etc;
- Redução do emprego de vigilantes em função da utilização de tecnologia eletrônica avançada, e do atendimento às exigências da legislação brasileira.

De acordo com esta mesma consultoria, os altos índices criminais encontrados hoje nas cidades brasileiras, tem causado profundos efeitos na sociedade e conseqüentemente nas empresas. Esta talvez seja, uma das principais razões para a saída de grande parte de empresas do Estado do Rio de Janeiro.

E em países do primeiro mundo? Quais seriam as ameaças percebidas pelos gestores de segurança das grandes empresas, como significativas aos seus negócios?

A empresa americana *Pinkerton*, a maior em serviços de segurança do mundo, que em 1999 comemorou 150 anos de vida, com um faturamento de 4 bilhões de dólares, vem realizando junto as empresas listadas na *Fortune* 1000, uma pesquisa que iniciou-se no ano de 1994.

Com o objetivo de criar uma importante ferramenta de gestão, a *Pinkerton* realizou entrevistas com os profissionais de segurança que estão à frente destas empresas, conseguindo coletar em 2002, 187 respostas em 17,3% das corporações.

Como poderemos observar, o resultado desta pesquisa nos revela que a maior preocupação dos profissionais e gestores de segurança destas empresas, está em seu público interno e não, como muitos imaginam, com o agressor externo. O trabalho da *Pinkerton*, é um dos mais importantes na atualidade, e deverá servir para alertar os profissionais brasileiros que estão preocupados com o muro de suas empresas, que a origem de seus riscos de maior criticidade, estará entrando todos os dias pela porta da frente.

A seguir, apresentamos o Quadro 01, onde estes profissionais listaram em ordem crescente de importância as vinte e três principais ameaças inerentes as suas empresas, com um respectivo grau de importância que variou de 01 (menos importante) à 05 (mais importante).

Em seguida, o Quadro 02, onde serão apresentados os resultados comparativos nos últimos 05 anos.

QUADRO 1

Colocação	Potenciais Ameaças	Grau importância
1	Violência no local de trabalho	4,02
2	Interrupção nos negócios/ recuperação de desastres	3,98
3	Terrorismo (global ou doméstico)	3,84
4	Crimes informatizados (intranet/ internet)	3,83
5	Seleção e contratação de funcionários	3,55
6	Fraudes e crimes do colarinho branco	3,41
7	Conduta não ética nos negócios	3,37
8	Roubo cometido por empregados	3,32
9	Crimes contra a propriedade	3,17
10	Drogas e álcool nas empresas	3,15
11	Processos e ações: Segurança inadequada	3,1
12	Roubo/ furto de hardware	3,1
13	Assédio sexual	3,05
14	Roubo de identidade	2,98
15	Gerenciamento e resposta à crises: Problemas de greve e instabilidade local	2,98
16	Roubo/ furto de software	2,97
17	Fraudes relacionadas a apólices de seguros de	2,91
18	Processo e ações: Negligência na contratação de funcionários	2,91
19	Espionagem empresarial: Roubo de informações	2,86
20	Gerenciamento e resposta à crises: Sequestro e extorsão	2,64
21	Gerenciamento e resposta à crise: Produtos contaminados e falsificação	2,58
22	Roubo de cargas	2,49
23	Desvio ilegal de produtos	2,32

Fonte: Pinkerton Top Security Threats - 2002

QUADRO 02

AMEAÇAS POTENCIAS	2002	2001	2000	1999	1998	1997
Violência no local de trabalho	1	1	1	1	2	1
Interrupção nos negócios/ recuperação de desastres	2	5	2	2	7	5
Terrorismo (global ou doméstico)	3	17	16	14	17	15
Crimes informatizados (intranet/ internet)	4	2	2	7	8	10
Seleção e contratação de funcionários	5	3	5	4	4	4
Fraudes e crimes do colarinho branco	6	4	4	3	3	7
Conduta não ética nos negócios	7	9	7	9	6	3
Roubo cometido por empregados	8	6	6	6	1	2
Crimes contra a propriedade	9	10	12	10	10	12
Drogas e álcool nas empresas	10	8	9	8	11	9
Processos e ações: Segurança inadequada	11	13	13	13	13	13
Roubo/ furto de hardware	11	7	8	5	5	6
Assédio sexual	13	11	10	11	14	14
Roubo de identidade	14	16	NA	NA	NA	NA
Gerenciamento e resposta à crises: Problemas de greve e instabilidade local	14	20	17	19	NA	NA
Roubo/ furto de software	16	7	8	5	5	6
Fraudes relacionadas a apólices de seguros de	17	15	15	16	19	17
Processo e ações: Negligência na contratação de funcionários	18	14	13	15	16	16
Espionagem empresarial: Roubo de informações	19	12	11	12	9	NA
Gerenciamento e resposta à crises: Sequestro e extorsão	20	19	18	18	NA	NA
Gerenciamento e resposta à crise: Produtos contaminados e falsificação	21	22	21	21	21	23
Roubo de cargas	22	18	19	17	NA	NA
Desvio ilegal de produtos	23	21	20	20	18	22

Fonte: Pinkerton Top Security Threats - 2002

NA- Ameaça não apontada no ano. Roubo de identidade começou a ser analisada em 2001.

Roubo de Hardware e Software foram pesquisados separadamente pela 1ª vez em 2002. Antes disso esta ameaça era considerada para a pesquisa de uma forma combinada.

Ao analisar os resultados da pesquisa, os especialistas da *Pinkerton* destacaram neste mesmo relatório, alguns pontos a serem observados, no que diz respeito as principais ameaças, à saber:

1) **Violência no Local de Trabalho**

Segundo Ray O' Hara, CPP (2002, p.3), a violência no local de trabalho que lidera a pesquisa nos últimos anos, será tornar-se mais grave depois do atentado de 11 de setembro.

De acordo com o especialista, as empresas terão o desafio de administrar também à partir de agora o nível de violência dos funcionários, no que diz respeito as suas diferenças étnicas. É importante salientar que a violência no local de trabalho, segundo Green (1998, p.474) poderá ser caracterizada por 04 eventos:

- 1) A ameaça, que poderá ser escrita ou verbal;
- 2) A sabotagem;
- 3) A agressão, usando a força física ou arma;
- 4) O constrangimento ou assédio;

2) **Interrupção nos negócios/ Recuperação de Desastres**

Segundo Dick Mc.Cormick, CPP (2002, p.4) com a nova ameaça do terrorismo global, o plano de continuidade de negócios deverá contemplar a total operação da empresa, em todas suas unidades. Acrescenta, que não se trata apenas de planos de contingência e exercícios de evacuação em caso de incêndio, e sim de

priorizar os tipos de operações nas instalações, determinando quais tem que ser trazidas de volta a operar em 8, 12, 24 ou 48 horas.

3) **Terrorismo**

David Fields, Vice-Presidente Sênior da *Pinkerton* Consultoria e Investigações (2002, p.4), ressalta que o grande desafio das empresas será proteger seus funcionários. Segundo sua análise, as empresas multinacionais e internacionais terão grande dificuldade em proteger seus executivos em trânsito ao redor do mundo, já que a ameaça terrorista não conseguindo atingir alvos governamentais, procurará naturalmente alvos menos protegidos.

4) **Segurança na internet/Intranet**

Dr. John Spain, CPP, CFE (2002, p.4), adverte as empresas que esta ameaça, pode atingir a todo tipo de empreendimento a qualquer hora e em qualquer lugar. Ressalta ainda, que o momento de maior vulnerabilidade será durante a integração de novas tecnologias.

De acordo com Spain, vivemos um momento de remover velhas tecnologias substituindo-as por novas, que naturalmente trarão novas ameaças.

Podemos concluir após estes resultados, que inúmeras ameaças sempre estarão presentes e nunca poderão ser totalmente eliminadas. A análise do ambiente indireto às empresas feita no Brasil, pela equipe da Brasiliano e Associados, é importantíssima em um primeiro momento, porque somente de posse de informações

relevantes como estas, poderemos selecionar as ameaças significativas ao nosso negócio.

A pesquisa realizada pela *Pinkerton*, revela um alto grau de consciência dos profissionais participantes, já que demonstra uma hierarquia bem definida das ameaças e suas conseqüências diretas e indiretas aos negócios das corporações.

Tudo isto, nos leva a refletir sobre a necessidade de romper com antigos paradigmas, herdados de nossos antecessores, e ver a nova área de segurança em formação, comprometida com a continuidade de negócios, a manutenção dos meios de produção e maior competitividade.

O foco principal deverá ser sempre a manutenção da vida e a redução de perdas empresarias, usando para isto meios de proteção e prevenção, que só poderão ser projetados, na medida em que se consiga desenvolver formas de percepção destas ameaças, e os impactos resultantes de sua materialização.

CAPÍTULO 04

3ª FASE DO PROCESSO DE ANÁLISE DE RISCOS

RECONHECENDO AS VULNERABILIDADES

De acordo com Carl Roper (1999, p.63), vulnerabilidade no processo de análise de riscos, é toda deficiência ou fraqueza capaz de ser explorada por um adversário, que tem como objetivo atingir os ativos de uma empresa. O autor explica que o processo para a tomada de consciência das vulnerabilidades, inicia-se nos primeiros contatos do analista de riscos com a empresa estudada, e continua durante a 1ª e 2ª fase do processo de análise de riscos.

Considero que o momento propício, para início desta fase em uma empresa é durante o processo de inspeção de segurança, onde serão coletados dados sobre a segurança física do local; segurança dos funcionários; proteção dos executivos; educação de segurança de todos os funcionários e visitantes; procedimentos em casos de emergências e desastres naturais; programas de manutenção de equipamentos; seguros; controle de acesso e divisão das áreas de segurança; segurança da informação, etc.

Carl Roper (1999, p.65), continua explicando que, durante a fase de revisão de dados da inspeção de segurança, existem alguns aspectos que serão muito importantes para o reconhecimento das vulnerabilidades, devendo ser observados:

- O propósito de existência da empresa analisada: missão, visão, valores, fatores

críticos de sucesso, objetivos e metas estratégicas;

- As políticas e procedimentos a serem seguidos na empresa;
- Descrição de cargos e responsabilidades de diretores e gerentes.

Segundo ele, a identificação das vulnerabilidades soluciona apenas parte do problema. Teremos que ser capazes também de identificar, se existem medidas de proteção e prevenção capazes de se contrapor a estas, em que proporção elas se apresentam, e quais são suas limitações.

O autor considera que para termos uma posição realista, deveremos analisar estas medidas realizando 07 perguntas, à saber:

1- Que tipo de proteção esta medida fornece?

Ex: Dissuadir, Impedir, Detectar, Atrasar etc.

2- Contra que tipo de evento indesejável ela atua?

Ex: Intrusão, Roubo, Sabotagem, fraude etc...

3- Durante quanto tempo do dia/ noite se mantém efetiva?

4- Qual a área coberta pela(s) medida(s)

5- Qual o histórico de mau funcionamento destas medidas?

6- Qual a correlação deste histórico, com os registros de eventos indesejáveis dentro da empresa?

7- Como é feita a manutenção destas medidas?

Como podemos observar, é muito importante toda a conceituação desenvolvida por Carl Roper sobre as vulnerabilidades no processo de análise de riscos. No entanto, devemos levar em consideração, que estas vulnerabilidades se originam na estrutura organizacional da empresa e em seu processo estratégico.

Segundo o relatório *Pinkerton* do ano de 1999, 8% dos departamentos de segurança se reportam aos *CEO's* das empresas e 26 % ao departamento de recursos humanos. Segundo os especialistas da *Pinkerton*, este tipo de estrutura, tem facilitado muito os programas de contratação de funcionários e de combate à violência no local de trabalho, mas limitam muito o restante das atribuições das equipes de segurança.

A *Pinkerton*, no entanto, observou em seu relatório do ano de 2000 que, as estruturas estão se modificando e a função de segurança está migrando dos departamentos de recursos humanos (26% em 1999 e 21% em 2000), para os departamentos jurídicos (11% em 1999 e 14% em 2000) e administrativo (7% em 1999 e 10% em 2000).

Segundo seus especialistas, estes departamentos tem uma maior influência dentro das estrutura organizacional das empresas, mas ainda assim, o desafio principal da segurança ainda será sensibilizar a alta gestão com suas recomendações.

O relatório do ano de 2002, nos revela agora, que o panorama acima citado ainda está longe de ser revertido rapidamente. Neste ano, a função de segurança continua se reportando fortemente ao departamento de recursos humanos (24%), com

ligeira elevação para o departamento administrativo (12%) e uma queda para o departamento jurídico (11%).

Com relação ao posicionamento estratégico, a situação é mais animadora, pois cada vez mais as empresas vem integrando a segurança em suas áreas estratégicas, como veremos no quadro abaixo:

QUESTÕES ESTRATÉGICAS	Ano de 2000		Ano 2002	
	SIM	NÃO	SIM	NÃO
<ul style="list-style-type: none"> Os planos operacionais dos departamentos de segurança estão em consonância com a estratégia corporativa das empresas? 	71%	29%	77%	23%
<ul style="list-style-type: none"> As empresas tem uma estratégia de segurança alinhada com o planejamento estratégico corporativo? 	56%	44%	60%	40%
<ul style="list-style-type: none"> As empresas tem participado de programas estruturados de qualidade? 	77%	23%	78%	22%

Fonte: Pinkeron Top Security Threats - 2001/2002

Tentamos demonstrar por meio de dados, que as vulnerabilidades das empresas no que concerne à área de segurança, são na verdade o produto de um processo que começa na maior parte das vezes, nos altos escalões das empresas. No cenário brasileiro, a falta de um planejamento estratégico corporativo, a inexistência de políticas de segurança formalizadas, a má formação dos profissionais e, em consequência disto a não integração de nossa área com as outras, ditas estratégicas, são os fatores determinantes para que sistemas operacionais sejam mau projetados e se tornem obsoletos.

Assim sendo, podemos começar a entender a origem dos problemas em nossa área nas corporações em todo o mundo, e não exclusivamente no Brasil, como muitos pensam. As vulnerabilidades, sempre serão a ponta do *iceberg*, que é o que pode ser vista acima da água. Só não podemos esquecer o que está abaixo dela.

CAPÍTULO 05

4ª FASE DO PROCESSO DE ANÁLISE DE RISCOS:

IDENTIFICAÇÃO, ANÁLISE E AVALIAÇÃO DE RISCOS

Estaremos iniciando agora o estudo da 4ª fase do processo de análise de riscos. Nesta fase, considerada por muitos profissionais a mais importante de todo o processo, é onde faremos uso das metodologias de análise e avaliação de riscos utilizados hoje, pelas escolas americanas e européias.

Como este estudo, tem o objetivo de se tornar também uma ferramenta de trabalho para os profissionais de segurança, procuramos captar na bibliografia existente o que há de mais efetivo nas duas linhas de pensamento.

Identificação dos Riscos

É muito importante inicialmente, entender como as duas escolas de pensamento atuam dentro do processo de análise de riscos. A escola americana valoriza todas as fases de uma forma equilibrada, atribuindo um mesmo valor a todas elas, como podemos observar pelos trabalhos de Roper e Broder.

Já a escola européia, tem seu foco em metodologias que utilizam critérios subjetivos de análise, disponibilizando em sua literatura apenas alguns comentários sobre a 1ª e 3ª fases do processo de análise de riscos. Esta escola, indica como ponto

de partida para a 4ª fase, a realização de uma matriz de riscos que identificará quais serão analisados, classificando-os em

grupos, com seus ativos correspondentes e possíveis danos, causados pela materialização destes riscos (Gómez – Merelo,1997, P.35). Esta matriz, encontra-se no **Anexo A**, desta monografia.

Esta matriz será muito importante, pois ajudará o analista a entender, que cada tipo de risco incide sobre um ativo determinado, como por exemplo: Roubo – bens e valores; chantagem / extorsão – pessoas; inundação – edifícios e instalações etc. Enfim, é preciso compreender que para todo o risco (agente causador do dano), existe um ativo correspondente (agente receptor do dano).

Outro estudioso da área de riscos, Antônio Celso Brasileiro, preconiza em sua metodologia de análise que na fase de identificação dos riscos é muito importante o conhecimento da origem destes. Seu método pode ser operacionalizado hoje, por meio de uma ferramenta informatizada chamada *Risk Net*.

Neste momento, o profissional de segurança terá que se dar conta, que poderá se deparar com um número muito grande de ativos. Neste caso poderá optar por fazer sua análise por área da empresa, o que acredito não ser o ideal.

Análise de Riscos

Existem inúmeros métodos de análise de riscos, sendo a maior parte deles defendido pela escola espanhola de Gomez – Merelo. A tabela abaixo aponta os principais, com suas aplicações específicas.

MÉTODO	APLICAÇÃO PRÁTICA
Método de Edwin E. Smith	Estabelecimento do grau de periculosidade de um determinado compartimento
Método de G. A. Herpol	Cálculo do risco de incêndios com base na carga térmica e resistência ao fogo dos elementos de separação
Método dos Fatores α	Determina a resistência e/ ou estabilidade ao fogo de um setor para confinar um incêndio em seu interior
Método dos Coeficientes K	Determina a resistência e/ ou estabilidade ao fogo de um setor para confinar um incêndio em seu interior
Método Proust	Calcula os componentes de risco do continente e do conteúdo para sua avaliação global
Método de Purt	Risco de incêndio e grau de proteção automática
Método de Cruzel Sarrat	Avaliação do risco de incêndio por cálculo (ERIC)
Método de Shibe	Instalações hospitalares
Método de Aschoff	Meios de proteção em função do risco
Método de Dow	Indústrias químicas
Método de Traubaud	Incêndios florestais
Método de Stadler	Localização de quartéis de bombeiros
Método de Pou	Localização de quartéis de bombeiros
Método de Grétener	Risco de incêndio
Método de Mosler	Avaliação do risco em geral

Fonte: Manual para El Director de Seguridad – 1997

Segundo Brasileiro (2002, p.45), o fator que determinará a escolha do método será o histórico dos riscos. Se a empresa possui um registro de suas ocorrências confiável, o que é bem raro, poderemos utilizar métodos estatísticos para o cálculo da probabilidade do risco acontecer. Esta metodologia encontra-se disponível no **Anexo B** deste trabalho.

Normalmente usaremos métodos subjetivos para análise, sendo o de Mosler o mais comum. Segundo Gómez – Merelo (1997,p.43), o método contempla 06 critérios para análise, à saber:

- 1- **Função**
- 2- **Substituição**
- 3- **Profundidade**
- 4- **Extensão**
- 5- **Agressão**
- 6- **Vulnerabilidade**

Para cada um dos critérios acima, serão atribuídos graus de 1 a 5 segundo suas tabelas específicas.

À partir de 1998, a escola espanhola divulgou por meio de seus manuais, uma reformulação no Método de Mosler, onde cada um dos critérios acima citados poderiam ser divididos em outros sub-critérios.

Este dimensionamento, permitiu uma redução na subjetividade do método.

As duas versões da Metodologia Mosler, encontram-se no **Anexo C** deste estudo.

Diferente da Metodologia Mosler de análise, que tem como objetivo final, a determinação de diferentes níveis para cada risco estudado, outro método,

desenvolvido por Willian T. Fine, é também amplamente utilizado, e determinará o grau de criticidade dos riscos.

Brasiliano (1999, p.132), esclarece que este método tem como objetivo principal estabelecer prioridades, determinando quais os riscos mais críticos e os menos críticos, permitindo que o departamento de segurança, defina o cronograma para a implementação das medidas de segurança juntamente com a previsão de investimentos.

O método T. Fine, é hoje utilizado como padrão pela Associação Americana de Gerenciamento de Riscos, sendo de importância fundamental no momento de justificar os investimentos, perante a alta gestão das empresas.

Assim como o método de Mosler, o método de Willian T. Fine é baseado em grades de probabilidades e avaliações subjetivas, e deverá ser utilizado quando a empresa não tem registros confiáveis sobre a materialização de seus riscos. O Método T. Fine consta no **Anexo D**, deste estudo.

Brasiliano, em sua metodologia de análise ainda nos revela, que uma análise de riscos eficiente, deverá ser capaz de coletar e analisar informações disponíveis ao ambiente direto e indireto à empresa estudada. Deverá projetar cenários, através de análises prospectivas. Segundo um dos maiores estudiosos brasileiros nesta área, Raul Grumbach (2002, p.34), uma das finalidades da prospectiva é propiciar uma visão global do ambiente e suas interligações.

Segundo Godet e Roubelat, 1996 citado pelo próprio Raul Grumbach (2002, p. 35)

“A prospectiva se propõem a iluminar as escolhas do presente com a luz dos possíveis futuros. Uma boa prospectiva, não é necessariamente aquela que se realiza, mas a que conduz a uma ação, evita os perigos futuros e atinge o objetivo desejado”.

Brasiliiano, continua explicando, que durante a de análise de riscos, assim como durante toda a atividade de planejamento nesta área, o profissional de segurança deverá ter uma visão do futuro, pois a prospectiva integra todas as variáveis que possam fazer com que os riscos se materializem.

Ressalta, que o horizonte temporal na realização da prospectiva de múltiplos cenários da área de riscos, deverá ser no máximo de um ano.

Avaliação de Riscos

Penúltima parte do processo de análise de riscos, a avaliação será fundamental para o profissional de segurança, pois é por meios de dados expressos nela, que será embasado todo o planejamento estratégico de segurança. Segundo Broader(2002, p.24), qualquer risco deverá ser descrito através de duas variáveis fundamentais.

A probabilidade de acontecer e os danos causados.

- **Probabilidade**

Quando a metodologia de análise for estatística, não haverá problema no cálculo da probabilidade. Devemos utilizar dados confiáveis para o cálculo da média, desvio padrão e coeficiente de variação, determinando então a probabilidade da média permanecer ou não.

A polêmica acontecerá justamente quando utilizarmos métodos subjetivos, como o de Mosler e T. Fine.

Brasiliano(2002, p.45), nos diz que é preciso parametrizar os métodos subjetivos de análise de risco. Segundo ele, devemos estabelecer faixas de probabilidade de modo empírico, no quadro final do Método de Mosler.

Quantificação do Risco	Nível do Risco	Probabilidade %
2 – 250	Muito baixo	0 – 20
251 – 500	Pequeno	20,1 – 40
501 – 750	Normal	40,1 – 60
751 – 1000	Alto	60,1 – 80
1001 - 1250	Muito alto	80,1 - 100

Fonte: Revista Proteger, Nov / Dez. 2002

Os intervalos de 20%, segundo o autor, também deverão ser divididos por 5(cinco), pois o critério da agressão, que mede a probabilidade do risco acontecer possui 05 níveis.

A nota dada neste critério, será o parâmetro para a quantificação exata da probabilidade, de forma que para uma nota 2 por exemplo, um risco de nível pequeno, utilizaremos a seguinte relação:

Nível: pequeno

Faixa de probabilidade aleatória: 20,1% - 40%

Dividindo a faixa em cinco níveis, teremos cada nível correspondendo a 4%.

Como a nota do critério de agressão é 2, em nosso exemplo, corresponderá então a:

$$2 \times 4\% = 8\%$$

Logo, segundo Brasiliano, a quantificação exata será:

$$Pb = 20,1\% + 8\% \therefore Pb = 28,1 \%$$

Em minha opinião, esta metodologia é questionável pois o Método Mosler tem 06 critérios de análise, e mesmo que se atribuisse o valor 5, nota máxima para a agressão, a classe

do risco estudado poderia ser classificada como **muito baixo**, o que colocaria o risco em uma faixa de probabilidade de 0 a 20%.

Isto seria uma contradição, pois não poderia ser considerado uma agressão muito alta, o risco que possuísse no máximo 20% de probabilidade de acontecer.

De acordo com Brasiliano, a mesma coisa poderá também ser feita com o método T. Fine.

Teríamos que dividir os 100% de probabilidade pelos três níveis de classificação, sendo:

QUANTIFICAÇÃO	NÍVEL DE CRITICIDADE	PROBABILIDADE%
Igual ou Maior que 200	Correção Imediata	66,68 – 100
Menor que 200 e maior que 85	Correção Urgente	33,34 – 66,67
Menor que 85	Monitoração	0 – 33,33

Fonte: Revista Proteger, Nov / Dez. 2002.

Cada faixa de probabilidade no caso, terá que ser dividida por seis, por que cada critério de análise de método T. Fine, consequência, exposição e probabilidade, apresentam seis níveis.

Cada uma das faixas então terá:

$$\text{Valor do Intervalo} = 33,33 / 6 = 5,56$$

Então, para um risco com criticidade igual 180, por exemplo, e com nota 3 na tabela do método, teremos:

$$GC = 180$$

$$\text{Faixa de probabilidade} = 33,34\% - 66,67\%$$

Considerando que a nota 3, corresponde ao quarto nível da tabela, teremos.

$$5,56 \times 4 = 22,24\%$$

Logo:

$$Pb = 33,34 \% + 22,24 \% = 55,58 \%$$

Assim como o Método de Mosler, o Método T. Fine também poderia sofrer algumas distorções, em minha opinião. A criticidade neste método, é representada pelo produto de três fatores: consequência, exposição ao risco e probabilidade de acontecer. No entanto, em uma análise onde a probabilidade fosse pequena e a consequência financeira fosse alta teríamos o risco em uma faixa de probabilidade alta, que seria outra contradição.

Acredito que o cálculo da probabilidade em métodos subjetivos, terá que ser no futuro reavaliado de forma mais profunda e detalhada, pois sua valoração é essencial para o processo de análise de risco.

- Perdas Empresariais e Relação Custo Benefício

Vimos até o momento, que quando usamos métodos subjetivos para análise de risco, entramos em um campo polêmico da área de segurança.

Visões diferenciadas dos diversos profissionais envolvidos no processo, poderão gerar muita polêmica e prejudicar os resultados alcançados. Será necessário que o gestor de

segurança, tenha muita tranquilidade ao conduzi-lo, e que exerça forte poder de liderança sobre sua equipe.

Citamos no início deste capítulo, o Método de Mosler, que tem o objetivo de classificar os diversos riscos em níveis ou graus.

O mesmo com o Método de Willian T. Fine, que estabelecerá a criticidade dos riscos, estabelecendo quais deverão ter prioridade em um programa de gestão de risco eficiente.

Demonstramos algumas formas, de se atribuir valores a probabilidade do risco acontecer partindo-se de métodos subjetivos, onde não é possível fazer uso da estatística.

Será necessário agora, que quantifiquemos os impactos negativos no negócio e o valor das perdas empresariais. É muito importante neste momento, a integração da área de segurança com toda empresa, por que quando se projetam perdas, não estamos somente nos referindo a perda financeira, mas sim todos os custos, diretos e indiretos que a empresa perde ou deixa de ganhar.

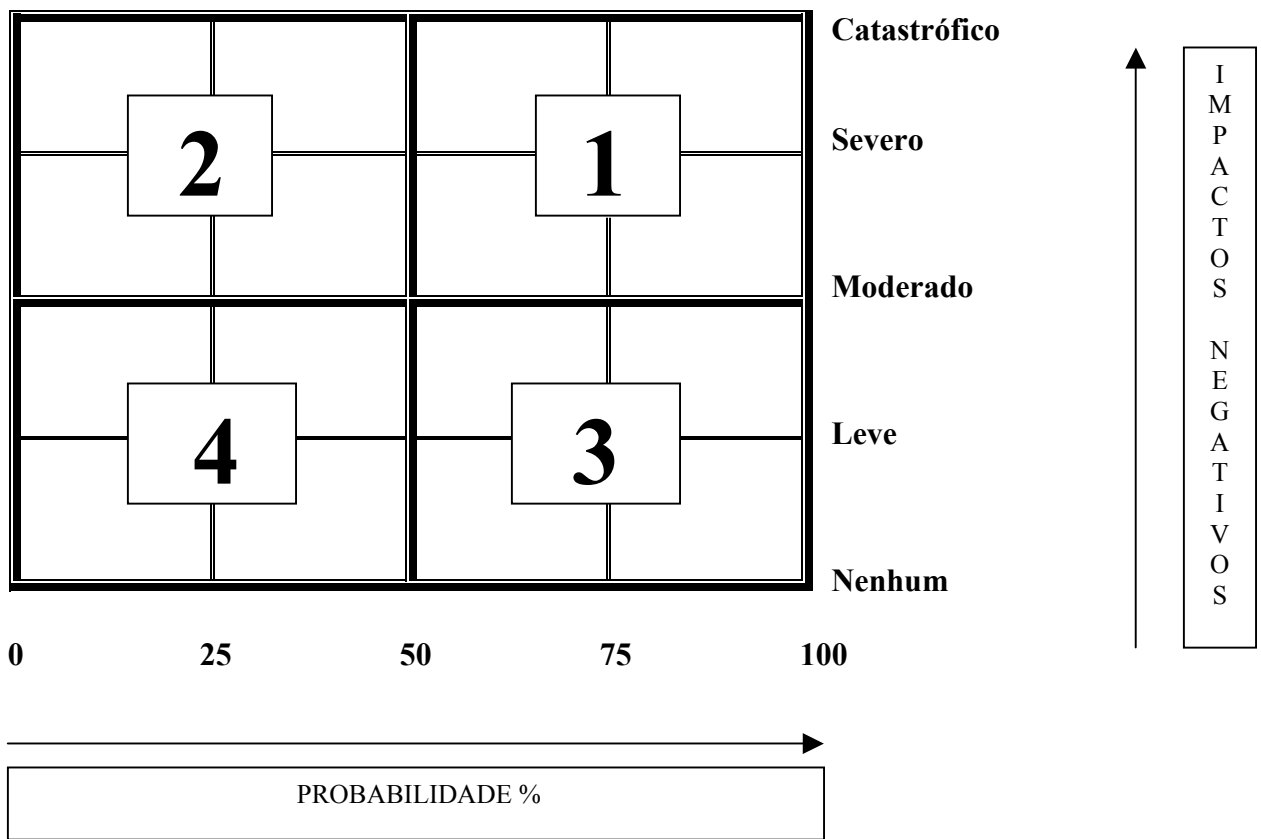
A integração destes dados, com a probabilidade do evento vir a acontecer demonstrará como resultado final, a vulnerabilidade da empresa perante os seus riscos. Esta, será a grande arma da segurança para conseguir investimentos em seu setor.

As formas para calcular as futuras perdas são inúmeras, indo desde aplicação de fórmulas até levantamentos *custom* dentro das empresas.

No **Anexo E** deste estudo, apresentaremos o modelo sugerido por Brasiliano(2000, p.58).

Seja qual for o processo utilizado, é crucial que ao final dos levantamentos fique bem claro para a corporação, a sua prioridade de investimentos, tendo em vista sua relação custo X benefício.

Para demonstração destes resultados, Brasiliano(2002, p.47), nos sugere uma matriz de vulnerabilidades dividida em quatro quadrantes, que terá em seu eixo vertical os valores das perdas empresariais, e no eixo horizontal o valores da probabilidade do risco acontecer. Então teremos:



Fonte: Revista Proteger, nov./dez. 2002

TRATAMENTO DOS RISCOS

Quadrante 1 – Riscos com alta probabilidade de ocorrência e impactos severos.

Exigem atenção imediata.

Quadrante 2 – Riscos com menor probabilidade de ocorrência e impactos severos.

Exigem monitoramento rotineiro.

Quadrante 3 – Riscos com alta probabilidade de ocorrência e impactos moderados.

Devem estar previstos no plano de contingência da empresa.

Quadrante 4 – Riscos com baixa probabilidade e impactos moderados.

Devem ser assumidos pela empresa.

Desta forma, a área de segurança poderá junto a empresa, estabelecer uma hierarquia dos riscos identificados, tratá-los e gerenciá- los adequadamente.

Brasiliano, completa sua explicação esclarecendo que o impacto negativo no negócio, terá que ser multiplicado pelo percentual correspondente para se obter e perda esperada.

Então teremos:

$$\text{PERDA ESPERADA} = \text{PB} \times \text{R\$}$$

Poderemos também, à partir do cálculo do grau de criticidade determinado através do método de Willian T. Fine, do percentual de riscos que queremos reduzir e do fator de custo, justificar nossos investimentos. Isto será possível, pela metodologia criada por R. Pickers, 1976, estabelecida como padrão pela Associação Americana de Gerenciamento de Riscos. O resumo do método Pickers está no **Anexo F**. desta monografia.

A matriz de Brasiliano, vista anteriormente, é essencial para as demonstrações feitas para a empresa e deverá ser completado pelo método de R. Pickers. A grande vantagem deste método, é que poderemos demonstrar a alta gestão da empresa qual o percentual de redução do risco, com o respectivo investimento. Estas informações integradas com a probabilidade do risco acontecer, e a valoração das perdas empresariais, deverão ser suficientes para validar as ações de nosso setor.

CAPÍTULO 06

A IMPORTÂNCIA DA GESTÃO DE RISCOS NAS CORPORAÇÕES

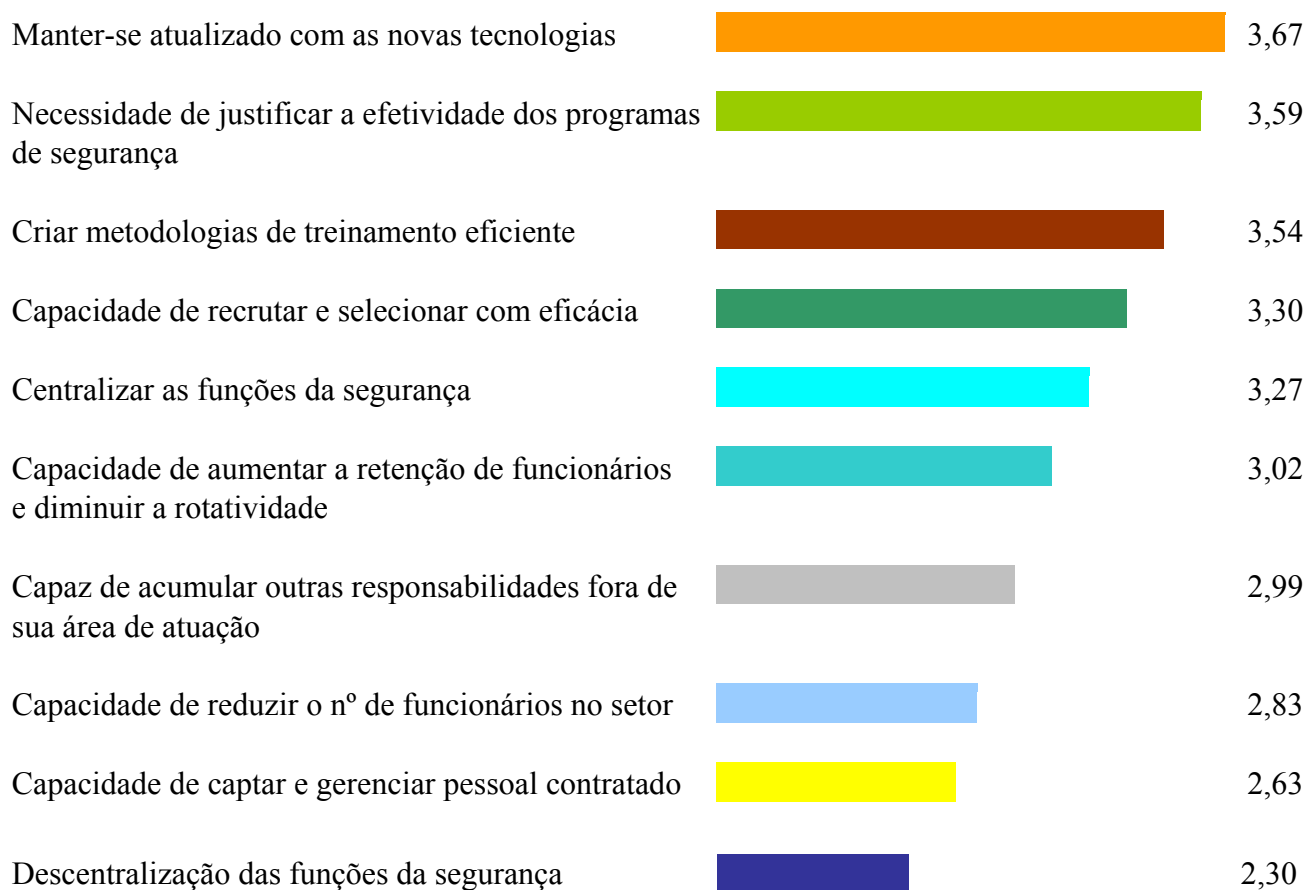
Com a chegada do novo milênio, e a quebra de vários paradigmas em todas as áreas de atuação das corporações, tornou-se necessário o despertar de novos conceitos na criação e gerenciamento de negócios. Verdadeiros gigantes corporativos ruíram, e pequenas empresas aglomeradas em escritórios tiveram lucros jamais imaginados, mostrando a todos que a concepção do “como ganhar dinheiro” mudou.

Como não poderia deixar de ser, dentro deste novo mundo, nasceu um novo profissional de segurança, também chamado de gestor de segurança, especialista em segurança, ou até em um conceito empresarial mais amplo, de *chief risk officer*. Os profissionais que não se acovardaram e embarcaram na nave da mudança, enfrentam hoje desafios inimagináveis, em um mundo dominado por uma violência descabida, desigualdades sociais intransponíveis e a busca do lucro nos negócios a qualquer preço.

E aqui estamos, no meio de tudo isto, com uma especialização que tem como missão fundamental proteger vidas, minimizar riscos, salvaguardar informações, colaborando para que as corporações continuem a ter lucratividade e competitividade ao longo dos tempos. Mais importante do que qualquer tipo de conhecimento, a ética deverá ser a companheira em todos os momentos.

Este novo gestor de segurança ou de riscos, deverá em seu dia a dia analisar tendências e ser capaz de projetar cenários futuros, que serão certamente construídos em cima de decisões presentes, criando para sua corporação uma maior previsibilidade sobre as ameaças existentes em seu ambiente direto e indireto.

O relatório de *Pinkerton*, 2002, define em sua pesquisa que, os maiores desafios na área de gerenciamento de segurança de uma forma geral são:



Segundo Roper (1999, p.99), quando focamos na área de gestão de riscos teremos as seguintes responsabilidades:

- Identificação do grau de exposição aos riscos sofridos pela corporação.
- Avaliação de riscos
- Gerenciamento dos riscos avaliados, dando ênfase à vida, patrimônio, meio ambiente e ao negócio.

- Formulação de um plano de emergência.
- Controle de contratos.
- Controle de orçamentos, junto com os departamentos de auditoria interna.

- Planejamento, implementação e controle de um programa de prevenção de perdas.

- Alimentar com dados o Planejamento Estratégico Corporativo, informando possíveis perdas acidentais.

- Administração, manutenção e proteção das informações.

Quando fazemos uma reflexão sobre as responsabilidades descritas acima, e os desafios da área de segurança para milênio, deduzimos que algumas questões serão fundamentais para a gestão de riscos. São elas:

Âmbito de Atuação

Normalmente, a área de gestão de riscos se preocupa com qualquer evento que possa causar perdas empresariais. Existem, no entanto, riscos chamados dinâmicos que são inerentes a administração dos negócios, que não são competência da área de segurança. A Equipe de *Redaccion de Editorial CPD*, SL(2001, p.122), que pertence a escola espanhola de segurança, nos esclarece quais são estes riscos:

- Riscos derivados de má gestão comercial.
- Riscos inerentes aos processos produtivos.
- Riscos inerentes a uma má gestão financeira.
- Riscos inerentes a decisões governamentais que afetariam diretamente a empresa.

Os autores nos esclarecem que, estes riscos, terão que ser gerenciados pelas outras áreas estratégicas da empresa. Os riscos de responsabilidade da área segurança, ou riscos puros, de acordo com escola espanhola, podem ser vistos no **Apêndice A**.

Empresas especializadas em gestão de riscos corporativos, como a consultoria Brasileiro e Associados, vem atuando em um espectro mais amplo, colocando também sob sua responsabilidade os riscos descritos acima.

Este posicionamento, segue em consonância com as novas tendências da gestão de riscos nos USA, que coloca o profissional de segurança como um *chief risk officer*, capaz de atender a toda corporação.

Tratamento dos Riscos

Diante de tudo que foi apresentado até o momento, será decisivo para o processo de gestão de riscos tratá-los cientificamente. Segundo Ficher e Green (1998, p.186), o tratamento dos riscos deverá ser feito de acordo com as necessidades da empresa, focada em seu próprio negócio e de acordo com seus valores essenciais. Para estes autores, a classificação de tratamento dos riscos deverá ser:

- a) Eliminar o risco – segundo os autores, tem-se que remover o problema para eliminar o risco. Isto poderá ser feito transferindo a responsabilidade para outro setor da empresa.
- b) Reduzir o risco – é reduzir os potenciais efeitos potenciais que este risco poderá causar.
- c) Transferir o risco – significa remover o risco da corporação, por meio de seguros.
- d) Assumir o risco – utilizado em casos em que os riscos tem baixa probabilidade de acontecer, e representam, por ocasião de sua materialização, danos empresariais moderados.

Para cada caso acima, corresponderá um nível de investimento. Caberá a alta direção da empresa, assessorada pela área de segurança esta decisão, que deverá ser embasada em todo processo de análise de riscos.

3 - CONCLUSÃO

Ao final deste trabalho, acredito ter alcançado meu objetivo final de realizar uma reflexão sobre o processo de análise de riscos, somando todas as informações disponibilizadas das duas escolas de segurança, identificando os valores a serem desenvolvidos pelos profissionais de nossa área.

Dentro deste campo da atuação, existem hoje dificuldades muito grandes geradas pela falta de experiência do nosso grupo; a falta de interação com a área de segurança pública, e em decorrência disto, a ausência de dados confiáveis; problemas de capacitação de nossos profissionais; a falta de bibliografia especializada e um maior aprofundamento científico.

Procurei enfatizar a fase de determinação dos ativos à proteger, pois auxiliar as empresas nesta escolha, será sem dúvida decisivo para a determinação das vulnerabilidades das empresas.

Destaquei também a importância da análise prospectiva na área de riscos, que ao se desenvolver, exigirá ainda mais do nosso gestor de segurança no que diz respeito a sua formação e aprendizado.

Finalmente, é muito importante dizer que o processo de análise de riscos a ser desenvolvido em uma corporação, deverá ser sempre personalizado. Ao cliente caberá sempre a palavra final sobre o que fazer com seus riscos, mas a longa caminhada até este momento caberá a nós, profissionais de segurança.

ANEXOS**ANEXO A****MATRIZ DE RISCO****ANEXO B****MÉTODO DAS PROBABILIDADES****ANEXO C****MÉTODO DE MOSLER****ANEXO D****MÉTODO DE WILLIAN T. FINE****ANEXO E****CÁLCULO DO CUSTO DAS PERDAS****EMPRESARIAIS****ANEXO F****MÉTODO DE R. PICKERS.**

ANEXO A

MATRIZ DE RISCOS

ANEXO B

MÉTODO DAS PROBABILIDADES

ANÁLISE DE RISCOS - MÉTODO DAS PROBABILIDADES

MÉTODO OBJETIVO:

- Probabilidade (P)
- Média (\bar{x})
- Desvio Padrão (S)
- Coeficiente de Variação (CV)
- Custo do Risco (CI)

PROBABILIDADE (P): É o número de vezes que um evento pode ocorrer, dividido pelo número de eventos.

$P = N/T$ P – probabilidade do evento ocorrer

N – número de vezes que o evento ocorre

T – número total de eventos

MÉDIA (\bar{X}): É o número médio de eventos em um determinado período.

$$\bar{X} = \frac{\sum X_i}{n} \quad \sum X_i - \text{somatório da frequência que o evento ocorre}$$

n – total de eventos

DESVIO PADRÃO (S): Determina em quanto a média deve variar

$$S = \sqrt{\frac{\sum (X_i - \bar{X})^2}{n}} \quad X_i - \text{frequência que o evento ocorre}$$

\bar{X} – média

COEFICIENTE DE VARIAÇÃO (CV) : Tem como resultado percentual a chance da estimativa diferir do resultado real.

A probabilidade do desvio estar correto é expressa da forma:

$$100 - CV = Y$$

$$Y / 100 = Y\%$$

$$CV = S / \bar{X}$$

ANEXO C

MÉTODO DE MOSLER

ANÁLISE DE RISCOS – MÉTODO DE MOSLER

DISPOSIÇÃO DOS CRITÉRIOS

Cada critério ou função estudado pode ser pontuado em uma escala que varia de 1 a 5 na pontuação dependendo de sua gravidade.

CRITÉRIO DA FUNÇÃO (F)

Critério que projeta as conseqüências negativas ou danos que podem alterar a atividade principal da empresa.

ESCALA	PONTUAÇÃO
MUITO GRAVEMENTE	5
GRAVEMENTE	4
MEDIANAMENTE	3
LEVEMENTE	2
MUITO LEVEMENTE	1

CRITÉRIO DA SUBSTITUIÇÃO(S)

Este critério avalia qual o impacto da concretização da ameaça sobre os bens, ou seja, o quanto os bens atingidos podem ser substituídos.

ESCALA	PONTUAÇÃO
MUITO DIFICILMENTE	5
DIFICILMENTE	4
SEM MUITAS DIFICULDADES	3
FACILMENTE	2
MUITO FACILMENTE	1

CRITÉRIO DA PROFUNDIDADE (P)

Uma vez materializado o risco, esse critério mede a perturbação institucional, os efeitos psicológicos e os danos à imagem da empresa.

ESCALA	PONTUAÇÃO
PERTURBAÇÕES MUITO GRAVES	5
GRAVES	4
LIMITADAS	3
LEVES	2
MUITO LEVES	1

CRITÉRIO DA EXTENSÃO(E)

Este critério mede o alcance e a extensão que o dano causa para a empresa

ESCALA	PONTUAÇÃO
CARÁTER INTERNACIONAL	5
CARÁTER NACIONAL	4
CARÁTER REGIONAL	3
CARÁTER LOCAL	2
CARÁTER INDIVIDUAL	1

CRITÉRIO DA AGRESSÃO (A)

Este critério mede a possibilidade do risco vir a se manifestar ,tendo em vista as características conjunturais e físicas da empresa,cidade e estado onde ela se encontra

ESCALA	PONTUAÇÃO
MUITO ALTA	5
ALTA	4
NORMAL	3
BAIXA	2
MUITO BAIXA	1

CRITÉRIO DA VULNERABILIDADE (V)

Tendo em vista o critério da agressão, este critério mede qual a probabilidade de que realmente se produzam danos ou perdas.

ESCALA	PONTUAÇÃO
MUITO ALTA	5
ALTA	4
NORMAL	3
BAIXA	2
MUITO BAIXA	1

ANÁLISE DE RISCOS - MÉTODO DE MOSLER

1. Critério da Função (F).

Critério que projeta as conseqüências negativas ou danos que podem alterar a atividade principal da empresa. Alteram a operação normal da entidade.

Os danos à imagem da entidade podem afetar:	
Muito gravemente	5
Gravemente	4
Medianamente	3
Levemente	2
Muito Levemente	1

Os danos nas instalações podem afetar:	
Muito gravemente	5
Gravemente	4
Medianamente	3
Levemente	2
Muito levemente	1

Os danos às pessoas (clientes e funcionários) da entidade podem afetar:	
Muito gravemente	5
Gravemente	4
Medianamente	3
Levemente	2
Muito levemente	1

2. Critério de Substituição(S).

Este critério avalia qual o impacto da concretização da ameaça sobre os bens, ou seja, o quanto os bens atingidos podem ser substituídos. Poderão ser substituídos por substituição física, duplicação técnica ou seguro.

O bem a ser substituído pode ser encontrado:	
No estrangeiro	5
No próprio país	4
Na região ou comunidade autônoma	3
Na província	2
No mesmo local	1

Para a reposição da infra-estrutura afetada, deve ser realizado:	
Uma obra geral	5
Uma grande obra local	4
Uma obra normal	3
Uma pequena obra	2
Não existe necessidade de obras	1

Os Trabalhos de substituição terão como prazo:	
Muito grande	5
Grande	4
Curto	3
Muito Curto	2
Imediato	1

Para que se realizem os trabalho de substituição serão necessários:	
Fechamento completo do negócio	5
Fechamento do negócio ao público	4
Trabalho em horário diurno	3
Pequenos trabalhos sem incomodar o público	2
Trabalho em horário noturno	1

3. Critério da Profundidade(P).

Uma vez materializado o risco, esse critério mede a perturbação institucional, os efeitos psicológicos e os danos à imagem da empresa.

Os danos à imagem da entidade em seu setor podem causar perturbações:	
Muito grandes	5
Graves	4
Limitadas	3
Leves	2
Muito leves	1

Os danos à imagem da entidade frente a seus clientes podem causar perturbações:	
Muito graves	5
Graves	6
Limitadas	3
Leves	2
Muito leves	1

Os dados à imagem da entidade percebida por seus funcionários podem causar perturbações:	
Muito graves	5
Graves	4
Limitadas	3
Leves	2
Muito Leves	1

4. Critério da Extensão(E).

Este critério mede o alcance e a extensão que o dano causou para a empresa.

O alcance das repercussões econômicas tem sido:	
Internacional	5
Nacional	4
Regional	3
Local	2
Individual	1

O alcance das repercussões dos danos à imagem da entidade tem sido:	
Internacional	5
Nacional	6
Regional	3
Local	2
individual	1

5. Critério da Agressão(A).

Este critério mede a possibilidade do risco se manifestar, tendo em vista as características conjunturais e físicas da empresa, cidade e estado onde ela se encontra.

Localização da agência ou sede da entidade:	
Situada isolada sem edifícios ao redor	5
Situada nos limites do polígono urbano	4
Situada no interior do polígono urbano	3
Situada no centro da cidade	2
Situada em um povoado ou vilarejo	1

Delinqüência na Zona:	
Zona de grande criminalidade	5
Zona de conflito social	4
Zona de criminalidade mediana	3
Zona de criminalidade baixa	2
Sem criminalidade	1

As forças de segurança do estado:	
Não patrulham a zona	5
Patrulham pouco a zona	4
Patrulham muito a zona	3
Batalhão a mais de 500m	2
Batalhão a menos de 500m	1

Vigilância nas instalações:	
Não existe	5
Não existe, mas há vizinhos	4
Existe em locais determinados	3
Existe vigilância noturna	2
Existe vigilância permanente	1

6. Critério da Vulnerabilidade(V).

Tendo em vista o critério da agressão, este critério mede qual a probabilidade de que realmente se produzam danos ou perdas.

Proteção perimetral:	
No existe nenhum tipo de proteção	5
Existem proteções físicas em mau estado	4
Existem proteções físicas em bom estado	3
Existem proteções físicas e eletrônicas em mau estado	4
Existem proteções físicas e eletrônicas em perfeito estado	1

Controle de acesso de funcionários e fornecedores:	
Não existe	5
Controle de acesso visual	4
Controle de acesso com identificação	3
Controle de acesso com identificação e verificação	2
Controle de acesso e de presença	1

Circulação de pessoas:	
Livre em todas as zonas sem identificação	5
Livre em todas as zonas com identificação	4
Controlado por zonas	3
Restringido por zonas	2
Proibido por zonas	1

MÉTODO DE MOSLER

1º Passo: Cálculo da Importância do Sucesso (I)

$$I = F \times S$$

F – nota do critério função

S – nota do critério substituição

2º Passo: Cálculo dos Danos Ocasionados (D)

$$D = P \times E$$

P – nota do critério profundidade

E – nota do critério extensão

3º Passo: Cálculo do Caráter do Risco (C)

$$C = I + D$$

4º Passo: Cálculo da Probabilidade (Pb)

$$Pb = A \times V$$

A – nota do critério agressão

V – nota do critério vulnerabilidade

5º Passo: Cálculo da Classe ou Nível do Risco (ER)

$$ER = C \times Pb$$

TABELA DE VALORAÇÃO DO RISCO

VALORES DE E.R.	CLASSE DO RISCO
ENTRE 2 E 250	MUITO REDUZIDO
ENTRE 251 E 500	REDUZIDO
ENTRE 501 E 750	NORMAL
ENTRE 751 E 1000	ELEVADO
ENTRE 1001 E 1250	MUITO ELEVADO

ANEXO D

MÉTODO DE WILLIAN T. FINE

MÉTODO DE WILLIAN T. FINE

OBJETIVOS

1. Determinar o grau de criticidade de riscos já devidamente analisados.
2. Trata-los de acordo com o resultado encontrado.
3. Integrar o grau de risco com a limitação econômica.
4. Direcionar os investimentos na área, entendendo que estes são diretamente proporcionais ao grau de criticidade.

FÓRMULA

$$\text{GRAU DE CRITICIDADE} = C \times E \times P$$

C – **Conseqüência** – impactos financeiros ou pessoais

E – **Exposição** – frequência que o evento ocorre na empresa ou em outras similares.

P – **Probabilidade** – é a chance real do evento vir acontecer.

TABELA G.C VALORES

FATOR	CLASSIFICAÇÃO	VALOR
CONSEQUENCIA C	a) Quebra da atividade-fim da empresa, dano superior a um milhão de dólares.	100
	b) Dano entre US\$ 500 mil e US\$ 1 milhão.	50
	c) Dano entre US\$ 100 mil e US\$ 500 mil.	25
	d) Dano entre US\$ 1 mil e US\$ 100 mil.	15
	e) Dano abaixo de US\$ 1 mil.	5
	f) Pequenos danos.	1
EXPOSIÇÃO E	a) Várias vezes ao dia	10
	a) Várias vezes ao dia.	10
	b) Uma vez ao dia – freqüentemente.	5
	c) Uma vez por semana ou ao mês – ocasionalmente.	3
	d) Uma vez ao mês ou ao ano – irregularmente.	2
	e) Raramente – sabe-se que ocorre, mas não com qual freqüência.	1
f) Remotamente possível, não se sabe se já ocorreu.	0,5	
PROBABILIDADE P	a) Espera-se que aconteça	10
	b) Completamente possível – 50% de chances.	6
	c) Coincidência se acontecer.	3
	d) Coincidência remota, porém possível.	1
	e) Extremamente remota, porém possível.	0,5
	f) Praticamente impossível de ocorrer, uma chance em	0,1

GRAU DE CRITICIDADE – G.C.	PRIORIDADES – AÇÕES A TOMAR
G.C. MAIOR OU IGUAL A 200	CORREÇÃO IMEDIATA – RISCO TEM QUE SER DIMINUÍDO
G.C. ABAIXO DE 200 E MAIOR OU IGUAL A 85	CORREÇÃO URGENTE – REQUER ATENÇÃO
G.C. MENOR QUE 85	RISCO DEVE SER MONITORADO

ANEXO E

CÁLCULO DO CUSTO DAS PERDAS EMPRESARIAIS

ANÁLISE DE RISCOS - CÁLCULO DO CUSTO DA PERDA

CUSTO DA PERDA (CP): mede o impacto financeiro com as perdas empresariais.

$$CP = SP + ST + CC - (I - P)$$

SP (Substituição permanente) – custos definitivos – equipamentos, instalações, salários, indenizações etc. que a empresa não obterá mais.

ST (Substituição temporária) – o que a empresa perde temporariamente – aluguel de equipamentos, instalação, tempo de funcionários parados.

CC (Custo conseqüente) – prejuízo dado à empresa – queda de faturamento, imagem.

I (Indenização do seguro) – quanto o seguro irá pagar em caso de sinistro.

P (Premio do seguro até o momento atual) – quanto se pagou em parcelas mensais à seguradora.

CUSTO DO RISCO (Ci): É a soma da proteção, do valor do seguro, e do que a empresa não coloca no seguro e nem protege.

$$Ci = Pi + Si + Vri \quad Ci - \text{custo de risco}$$

Pi – valor gasto em proteção

Si – valor gasto em seguro

Vri – valor do risco

i – momento (mês, semana, ano)

$$VR = P \times M \quad VR - \text{valor do risco}$$

P – probabilidade

M – magnitude

ANEXO F

MÉTODO DE R. PICKERS

JUSTIFICATIVA DE INVESTIMENTO

MÉTODO DE PICKERS

OBJETIVO

Determinar se o gasto proposto no investimento de segurança é justificável.

FÓRMULA

GRAU DE CRITICIDADE

$$JI = \frac{\text{FATOR DE CUSTO X GRAU DE CORREÇÃO}}{\text{GC}}$$

FATOR DE CUSTO X GRAU DE CORREÇÃO

GC – Grau de Criticidade – já analisado anteriormente.

Fator de Custo – valor do investimento em segurança – número na tabela correspondente.

Grau de Correção – percentual do risco tratado – número na tabela correspondente.

OBS: O valor de JI, deverá ser analisado na tabela ESCALA DE VALORAÇÃO DE PICKERS

FATOR DE CUSTO	
CLASSIFICAÇÃO	VALOR
MAIOR QUE US\$ 50.000	10
ENTRE US\$ 25.000 E US\$ 50.000	6
ENTRE US\$ 10.000 E US\$ 25.000	4
ENTRE US\$ 1.000 E US\$ 10.000	3
ENTRE US\$ 100 E US\$ 1.000	2
ENTRE US\$ 25 E US\$ 100	1
MENOS QUE US\$ 25	0,5

GRAU DE CORREÇÃO	
CLASSIFICAÇÃO	VALOR
RISCO ELIMINADO – 100%	1
RISCO REDUZIDO – 75%	2
RISCO REDUZIDO ENTRE – 50% E 75%	3
RISCO REDUZIDO ENTRE 25% E 50%	4
RISCO REDUZIDO MENOR QUE 25%	6

ESCALA DE VALORAÇÃO DO ÍNDICE DE JUSTIFICAÇÃO	
FATOR ÍNDICE DE JUSTIFICAÇÃO IJ	COMENTÁRIOS
IJ MENOR QUE 10	INVESTIMENTO DUVIDOSO
IJ ENTRE 10 E 20	INVESTIMENTO NORMALMENTE JUSTIFICADO
IJ MAIOR QUE 20	INVESTIMENTO PLENAMENTE JUSTIFICADO, GRANDE REDUÇÃO DE RISCO

5 - BIBLIOGRAFIA

BINTHIFF, Russel L. The Complete Manual of Corporate and Industrial Security. Englewood: Prentice Hall, 1992

BRODER, James F. Risk Analysis and the Security Survey.

Boston: Butterworth – Heinemann, 2ª edição, 2000

BRASILIANO, Antônio Celso Ribeiro. Planejamento de Segurança Empresarial- Metodologia e Implantação. S.Paulo, Cia. Das Artes, 1999.

BRASILIANO, Antônio Celso Ribeiro. Risk Net: Aumentando a Eficácia no Monitoramento. Revista Proteger, S.Paulo, número 41, pg. 40 à 48, 2002.

EDITORIAL CPD, SL. Directores de Seguridad: Analisis y Gerencia de Riesgos. Madrid, Imprico-Imprenta Comercial, 2000.

FISHER, Robert e GREEN, Gion. Introduction to Security.

Boston: Butterworth – Heinemann, 6ª edição, 1998.

GOMEZ-MERELO, Manuel Sánchez. Manual para el Director de Seguridad. Madrid, GET, 2ª edição, 1997.

GOMEZ-MERELO, Manuel Sánchez. Seguridad em Entidades Bancarias: Munual para Proyectos e Gestion. Madrid, GET, 2ª edição, 1998.

HAROWITZ, Sherry L. The New Centurions. Revista Security Management, EUA, número 1 pg 51 à 58, 2003.

MARCIAL, Elaine Coutinho e GRUMBACH, Raul José dos Santos. Cenários Prospectivos: Como Construir um Futuro Melhor. Rio de Janeiro: Editora FGV, 2002.

MARCY, José de Campos Verde. Foco na Gestão da Segurança Empresarial . Revista Proteger, S.Paulo, número 31, pg. 41 à 43, 2000.

PINKERTON CONSULTING and INVESTIGATIONS. Top Security Threats and Management Issues Facing Corporate America 2002 Survey of Fortune 1000 Companies, Pinkerton Service Corporation, 2002.

PURPURA, Philip. Security and Loss Prevention : An Introduction. Boston: Butterworth – Heinemann, 3ª edição, 1998

SENNEWALD, Charles A. Effective Security Management
Boston: Butterworth – Heinemann, 3ª edição, 1998

ROPER, Carl A. Risk Management for Security Professionals. Boston: Butterworth – Heinemann, 1999.