# Coletânea Gestão de Riscos Empresariais

Cláudio dos Santos Moretti

# Coletânea Gestão de Riscos Empresariais

Cláudio dos Santos Moretti

CES - ASE

Moretti, Cláudio dos Santos.
Coletânea Gestão de Riscos empresariais. USA. Monee, Illinois. Editora: Independently published. 2020.
ISBN: 9798673856420

# SUMÁRIO


..... 0

PREFÁCIO ..... 3

SOBRE O AUTOR ..... 4

RISCOS GLOBAIS PARA OS PRÓXIMOS 10 ANOS ..... 5

ISO 31000 – NORMA DE GESTÃO DE RISCOS ..... 12

GESTÃO DE RISCO, A NOVA NORMA DA ABNT ..... 16

QUAL A IMPORTÂNCIA DA GESTÃO DE RISCO NO PLANEJAMENTO DA SEGURANÇA ..... 18

A IMPORTÂNCIA DA GESTÃO DE RISCO NO TRANSPORTE DE CARGAS ..... 20

GESTÃO DE RISCO - IDENTIFICAÇÃO DOS RISCOS E FATORES DE RISCO ..... 23

DIAGNÓSTICO DE SEGURANÇA ..... 30

METODOLOGIA PARA ANÁLISE DE RISCOS – MÉTODO ESTATÍSTICO (ATUALIZADO) ..... 37

MÉTODOS DE ANÁLISE DE RISCO – MÉTODO MOSLER (ATUALIZADO) ..... 45

MÉTODO DE ANÁLISE DE RISCO – T. FINE ..... 54

MÉTODO BRASILIANO (BÁSICO) PARA ANÁLISE DE RISCOS ..... 65

PLANEJAMENTO TÁTICO DE SEGURANÇA ..... 75

PLANEJAMENTO TÁTICO - ELABORAÇÃO DO PLANO DE AÇÃO ..... 85

REFERÊNCIAS ..... 90

# PREFÁCIO

Este material foi elaborado a partir das diversas publicações pelo autor no Jornal da Segurança, na Revista Gestão de Riscos e do SESVESP com temas relacionados à Gestão de Riscos Empresariais;

Os artigos sofreram pequenos ajustes a fim de atualiza-los sobre os temas e, principalmente por conta da publicação da ISO/NBR 31000 e 31010, nos casos dos artigos que foram publicados antes destas normas.

Também foram editados em sequência mais sistêmica com o objetivo de facilitar o entendimento e não na ordem cronológica em que foram publicados.

O objetivo deste material é auxiliar o gestor de segurança iniciante, principalmente, para desenvolvimento e aprofundamento nesta matéria, com conceitos e apresentação de alguns métodos de análise de riscos que possibilitem a elaboração de um plano tático de segurança da sua área de atuação, haja vista que a gestão de riscos é aplicável a qualquer tipo de negócio.

Além do plano de segurança, após a análise e avaliação dos riscos, poderá ser utilizado, de acordo com o negócio e apetite ao risco, para a elaboração dos planos de emergências e/ou de continuidade do negócio.

Boa leitura!

# SOBRE O AUTOR

**Ex-sargento** do Exército (1980-1987); Graduado em Gestão Empresarial – UNIMONTE – Santos (2003) e Tecnólogo em Processos Gerenciais - FAEL. Especializado em **Gestão da Segurança Empresarial** – MBA - FECAP/Brasiliano; Pós-graduado em **Gestão de Crises Corporativa**, - Universidade Gama Filho; Pós-graduado em **Inteligência Estratégica** - AVM; MBA em **Gestão da Qualidade**; MBA Executivo em **Gestão de Pessoas**; Gestión de Seguraridad Empresarial Internacional pela **Universidad Pontificia Comillas**, realizado em Madri, ES; Especialista em Gestón del Riesgo pelo **IUGM** – Instituto Universitário General Gutiérrez Mellado de la UNED Centor de Estudios de Seguridad (GET). Diversos cursos de extensão universitária. Professor da **FAPI/FESP-SP/Brasiliano INTERISK** no Curso Avançado em Segurança Empresarial – **MBS**, (2005 – 2019); foi professor do Curso de Gestão em Segurança da Universidade Monte Serrat (2005 – 2008) – **UNIMONTE**; foi professor do Curso Graduação Tecnológica de Gestão em Segurança Privada - **UNIP/Santos** (2009 – 2016); **Autor de sete DVDs** sobre segurança, editados pelo **Jornal da Segurança**; Articulista em diversas revistas especializadas com mais de **100 artigos publicados**. Trabalhou na **Petrobras**, (1987 – 2016) no setor de Inteligência e Segurança Corporativa (aposentado - 10/2016); Foi Coordenador da **Escola Falcão** – Centro de Formação e Treinamento de Segurança – Santos – SP (1999 – 2008); Membro da Associação dos Diplomados da Escola Superior de Guerra (ADESG); Perito judicial em gestão empresarial. Autor de **dois livros** didáticos da **KROTON Educacional** para cursos presenciais e EAD de Gestão de Segurança Privada nas universidades: Segurança bancária e transporte de valores, 2017. - Negociação e gestão de conflitos de segurança, 2018. Certificado de Administrador de Segurança Empresarial (**ASE**) pela Associação Brasileira dos Profissionais de Segurança Empresarial – ABSEG; Certificado de Especialista em Segurança Empresarial (**CES**) pela Associação Brasileira de Segurança Orgânica – ABSO; Professor em diversos cursos do **SESVESP** – (2013 – 2019). Autor de 12 cursos EAD para **IBRAGESP**; 03 para **Senhora Segurança**; 01 para **KROTON** e 01 para **ABSEG**.

## RISCOS GLOBAIS PARA OS PRÓXIMOS 10 ANOS

No início deste ano o Fórum Econômico Mundial de Davos publicou sua nona edição do relatório Riscos Globais 2014 (Global Risks 2014), tendo uma perspectiva de 10 anos, o relatório avalia 31 riscos que são de natureza global e têm o potencial de causar impacto negativo significativo em todos os países e indústrias.

Os riscos são agrupados em cinco categorias - econômica, ambiental, geopolítica, social e tecnológica - e medidos em termos da sua probabilidade e seu impacto potencial.

O Fórum - Fórum Econômico Mundial é uma organização internacional independente cujo objetivo é “melhorar a situação do mundo” mobilizando líderes empresariais, políticos e a sociedade. O Fórum é reconhecido por sua conferência anual em Davos, Suíça, onde membros e líderes mundiais discutem vários desafios globais. Com matriz em Genebra, a organização foi fundada como Fórum Europeu de Gerenciamento, em 1971 por Klaus, professor de administração na Suíça e atual presidente do Fórum. Passou a se chamar Fórum Econômico Mundial em 1987, após expandir seu projeto para incluir a resolução de conflitos internacionais.

Neste ano, chama a atenção à identificação da interconectividade entre os riscos.

O relatório analisou 31 riscos para os próximos dez anos. Os principais riscos que os participantes do fórum identificaram foram as crises orçamentais nas principais economias, o desemprego ou subemprego estruturalmente alto, as crises da água, o fracasso na adaptação e mitigação das alterações climáticas e da governança global, as crises de alimentos, a falha nas maiores instituições e mecanismos financeiros, além da profunda instabilidade política e social.

Estes riscos foram identificados por políticos, acadêmicos e empresários, que só poderão ser enfrentados com "cooperação internacional", justamente devido a interconectividade dos riscos analisados.

Essas interconexões não representam a causalidade direta. Elas são, provavelmente, indiretas, por exemplo, através dos impactos paralelos ou da compensação da mitigação.

As interconexões de riscos globais mostram como todos os riscos globais são conectados uns aos outros e define a complexidade de se lidar com o risco global de uma forma eficaz.

Isso demonstra a força da conexão entre os riscos individuais - os riscos mais fortemente conectados poderiam merecer atenção adicional devido às múltiplas formas que afetam ou são afetados por outros riscos.

E o que isso quer dizer? Bem, os riscos, assim como as coisas que acontecem no nosso mundo, sejam elas econômicas ou de doenças elas estão todas interconectadas. Hoje quase não há endemias, mas epidemias, com risco de virar uma pandemia. Apenas para entender: a endemia é relacionada a uma doença de uma determinada área ou região, como a febre amarela, por exemplo. A epidemia refere-se a uma doença contagiosa que espalha com facilidade como por exemplo, o ebola. Já a pandemia é uma epidemia que atinge grandes proporções, podendo se espalhar por um ou mais continentes ou por todo o mundo, causando inúmeras mortes ou destruindo cidades e regiões inteiras, como por exemplo, a Gripe Suína H1N1.

Dessa forma, o efeito borboleta, que faz parte da teoria do caos, ganha força, principalmente pela interconexão entre todos os países do planeta e

consequentemente dos riscos potenciais desta globalização, onde os riscos cibernéticos (hiperconectados), a desigualdade social e o clima, para citar apenas alguns, nunca haviam validado, de maneira mais urgente e necessária, a velha máxima de pensar globalmente e agir localmente.

Apenas para citar um dos riscos potenciais e o impacto que ele traz, veja o que o diz o resumo do relatório Perdas líquidas: estimativa do custo global do cibercrime - Impacto econômico do cibercrime elaborado pela McAfee:

“O cibercrime é uma indústria em crescimento. O retorno é grande e os riscos são baixos. Estimamos que o custo anual do cibercrime para a economia global excede US$ 445 bilhões, incluindo tanto os ganhos para os criminosos quanto os custos das empresas com recuperação e defesa. Uma estimativa conservadora seria de US$ 375 bilhões em perdas, enquanto o máximo poderia chegar a US$ 575 bilhões. Isso é mais do que a renda nacional da maioria dos países e o equivalente a algo entre 0,5% e 0,8% da renda mundial”.

Você ainda duvida que todos nós estamos interconectados?


## Qual a importância da análise de risco para o profissional de segurança (atualizado)

"Se tens um fenômeno que não entendes, para que possa entendê-lo deves pegar uma régua e medi-lo. Se não existe uma régua para medir o fenômeno, inventa uma, mede o fenômeno e então entenderás". Galileu Galilei

As diversas experiências de profissionais da segurança empresarial têm demonstrado que uma das ferramentas mais procuradas hoje em dia são as metodologias para a realização de uma análise de risco.

E este crescente aumento no interesse destas metodologias tem uma justificativa muito plausível - as metodologias para análise de risco têm separado o "joio do trigo" no segmento de profissionais da segurança privada.

Até bem pouco tempo era muito comum a falta de profissionalismo nesta área, hoje a situação está muito melhor e com tendência de aumento do nível profissional.

Hoje as universidades têm cursos de gestão de segurança, preparando o futuro gestor de empresas de segurança. Existem cursos de extensão universitária neste segmento, cursos de pós-graduação (MBA) de gestão de segurança, alguns países que têm a sua formação de profissionais de segurança mais antigas já se apresentam para trazerem cursos para o Brasil, além de grupos de profissionais que saem em busca de informações atualizadas em cursos na Europa e nos EUA.

Enquanto isso, continua no Congresso, o projeto de Lei que fará alterações significativas na Lei 7.102/83 (conhecido como Estatuto da Segurança Privada)

que dispõe sobre a criação do gestor de segurança, no qual conceitua o gestor de segurança privada como profissional especializado, de nível superior, que, de acordo com o Art. 26, terá as seguintes responsabilidades:

Fazer análise de riscos e definição e integração dos recursos físicos, humanos, técnicos e organizacionais a serem utilizados na mitigação de riscos;

Elaborar projetos para a implementação das estratégias de proteção; e realizar auditorias de segurança em organizações públicas e privadas.

Tudo isso demonstra que estamos no caminho certo, ainda que a passos lentos, e um grande diferencial que já se observa é justamente com relação a análise de risco, seja ela estratégica, tática ou operacional, todas têm seus valores e medidas adaptadas a cada situação.

E o motivo deste crescimento na busca das melhores metodologias de análise de risco é porque ela traz um diferencial enorme em qualquer projeto de segurança. Ela dá a verdadeira dimensão dos riscos que a empresa está sujeita.

O que a análise de risco procura responder é qual a chance de uma empresa sofrer um sinistro e qual o impacto financeiro e/ou operacional ele pode causar.

Além disso o profissional de segurança saberá qual a perda esperada e consequentemente qual o valor máximo que ele poderá investir para mitigar determinado risco.

A análise de risco é, para o profissional de segurança, uma ferramenta importantíssima que poderá identificar os riscos que a empresa está sujeita e os fatores de risco que expõe a empresa à concretização destes riscos.

O resultado desta análise mostrará onde ele deve agir, atuando diretamente nas causas para evitar seus efeitos.

Poderá criar seu plano de ação a partir do resultado da análise de risco, criar metas para serem atingidas, poderá criar mecanismos de controle para acompanhar todo o desenrolar do plano de ação, ajustando-o conforme for o mais adequado, sem desviar-se das metas pré-estabelecidas.

Lembrando que a finalidade da segurança corporativa é dar condições para que a empresa possa prosperar, manter-se competitiva e preocupar-se com a sua atividade fim e não com os empecilhos e prejuízos que a falta de segurança pode trazer.

O mais importante é o negócio e não a segurança.

O gestor poderá monitorar os riscos e dar a atenção adequada de acordo com a situação e a evolução de cada risco.

Sempre haverá riscos residuais, pois, a segurança absoluta não será possível, portanto, estes riscos residuais devem ser identificados, estimados e monitorados.

Não existe risco zero.

Com base na análise de riscos, o gestor poderá identificar a necessidade de preparar seu plano de contingência para os riscos que tenham maior impacto.

A análise de risco nos ajuda a identificar os ativos da empresa, sejam eles tangíveis ou intangíveis, pois todos necessitam de proteção adequada, principalmente quando se trata de uma análise de risco estratégica.

Das metodologias existentes, podemos dividi-las em três tipos, as objetivas/quantitativas, as subjetivas/qualitativas ou uma combinação destas alternativas. Mas qual seria a melhor?

Na metodologia objetiva, nós não podemos influenciar, não podemos adequá-la aos fatos presentes, principalmente quando ela tem um histórico muito antigo ou muito longo, pois é como se acreditássemos que nada mudou nos últimos anos e nada mudará daqui para a frente, seguindo a mesma tendência, sem que as circunstâncias atuais sejam levadas em consideração.

Ele é matemático e por isso não podemos atualizá-lo, mesmo que nós tivéssemos informações para isso, pois faltaria histórico, ou seja, fatos que já aconteceram e nada se pode fazer para atualizarmos estes dados até que eles formem outro histórico, dessa forma, teremos que esperar para poder atuar neste resultado. Agiremos reativamente.

Já no caso das metodologias subjetivas/qualitativas, a opinião do profissional de segurança é fundamental para termos uma matriz mais realista, tanto em relação as probabilidades como aos impactos no negócio, e este resultado depende da experiência do profissional de segurança, da equipe que trabalhou na elaboração da análise, das informações disponíveis e busca uma visão mais atualizada e de futuro, pois a ideia é agir de maneira preventiva, evitando a concretização de um risco real ou potencial.

Para o empresário, a análise de risco traz informações que irão auxiliá-lo na tomada de decisão de onde investir a fim de reduzir os riscos, onde está ocorrendo sua perda e até para decidir se vai assumir o risco, se vai transferi-lo, eliminá-lo ou autofinanciá-lo.

De acordo com a decisão tomada, serão aplicadas as medidas de segurança, através do plano de ação, que traduzirá esta decisão para a forma de atuação da segurança.

A decisão cabe aos responsáveis pelo negócio e não ao gestor de segurança.

Além disso, para o empresário, a análise de risco traz mais confiabilidade ao projeto de segurança que até bem pouco tempo era (e na maioria dos casos ainda o é) encarado como gastos e não como investimento, totalmente separado dos demais departamentos, como uma função e não como um processo, que deve estar integrado a todos os demais processos das empresas, daí a necessidade de atualização constante, buscando o melhor resultado para a empresa.

Para isso é necessário apresentar resultados financeiros, mostrar retorno nos investimentos feitos na segurança, apresentando um projeto viável, que tenha valores exequíveis que possam ser mensurados, matriciados e acompanhados.

É, na verdade, inserir a segurança no mesmo contexto dos demais departamentos da empresa, seja financeiro, de produção, manutenção, etc. A segurança também precisa cumprir metas e ajustar-se às exigências do mercado e essa história ainda está sendo escrita.... Por todos nós.


## ISO 31000 – NORMA DE GESTÃO DE RISCOS

A ABNT – Associação Brasileira de Normas Técnicas é o foro nacional de normalização, ou seja, é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro. De acordo com a ABNT, Norma é um documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto.

Agora chegou a vez da gestão de riscos que, desde que os gestores começaram a utilizar esta ferramenta no Brasil, tem havido divergências com relação, principalmente, dos conceitos sobre o tema.

Os métodos de análise de risco continuarão exercendo sua função, sendo que um pelo menos já apresenta convergência com a norma de gestão de riscos, o método Brasiliano avançado de análise de riscos corporativos.

A primeira edição da norma brasileira de gestão de riscos – ABNT NBR 31000/2009 foi lançada, em 30/11/2009, entrando em vigor a partir de 30/12/2009. A versão brasileira tem as mesmas premissas e orientações da ISO americana. A ISO 31000 que a ABNT – Associação Brasileira de Normas

Técnicas aprovou para uso no Brasil foi baseada na norma AS/ NZS 4360, norma de gestão de risco utilizada na Austrália e na Nova Zelândia.

A norma AS/NZS 4360 foi publicada em 1995, tendo sofrido uma revisão em 1999 e outra em 2004 e era considerada a mais completa, sendo usada como base da ISO 31000.

Também é importante conhecer a terminologia utilizada na Norma. Neste caso, ainda em 30/11/2009 a ABNT publicou a ABNT ISO GUIA 73, que substitui a ABNT ISO/IEC GUIA 73/2005, que foi revisada. O Guia 73/2009 traz o vocabulário básico para podermos entender e falarmos a mesma língua em relação à gestão de risco. Daí a importância deste Guia.

Ao contrário do que muitos imaginavam a norma não será utilizada para certificação e não é de uso obrigatório.

Segundo a própria ABNT, as Normas Brasileiras são desenvolvidas e utilizadas voluntariamente e tornam-se obrigatórias somente quando explicitadas em um instrumento do Poder Público (lei, decreto, portaria, normativa etc.) ou quando citadas em contrato.

Ela também não traz um método de análise de risco, ela apresenta uma estrutura para a gestão de risco, fornece uma abordagem comum em apoio às demais normas, sem substituí-las.

Como vimos, a ISO 31000 não será de uso obrigatório ou utilizada para certificação, porém será referência para os gestores e tenderá a unificar a linguagem, conceitos e estrutura de uma gestão de risco, portanto seu conhecimento e aplicação serão impostos pela própria comunidade da segurança que agora tem uma referência internacional de gestão de riscos.

Para apoiar a ISO 31000, no dia 01 de dezembro de 2009, entrou em vigor a norma ISO/IEC 31010:2009 “Risk management – Risk assessment techniques” ou Gestão de riscos – Técnicas de avaliação de riscos, que fornece orientação sobre a seleção e aplicação de técnicas sistemáticas de avaliação de riscos, não trata particularmente de questões de segurança.

É uma norma genérica de gestão de riscos e todas as referências à segurança que existem no documento são de natureza informativa e ainda não tem previsão para publicação, pela ABNT no Brasil.

A ISO 31000 é descrita de forma genérica e fornece os princípios e diretrizes para gerenciar qualquer forma de risco.

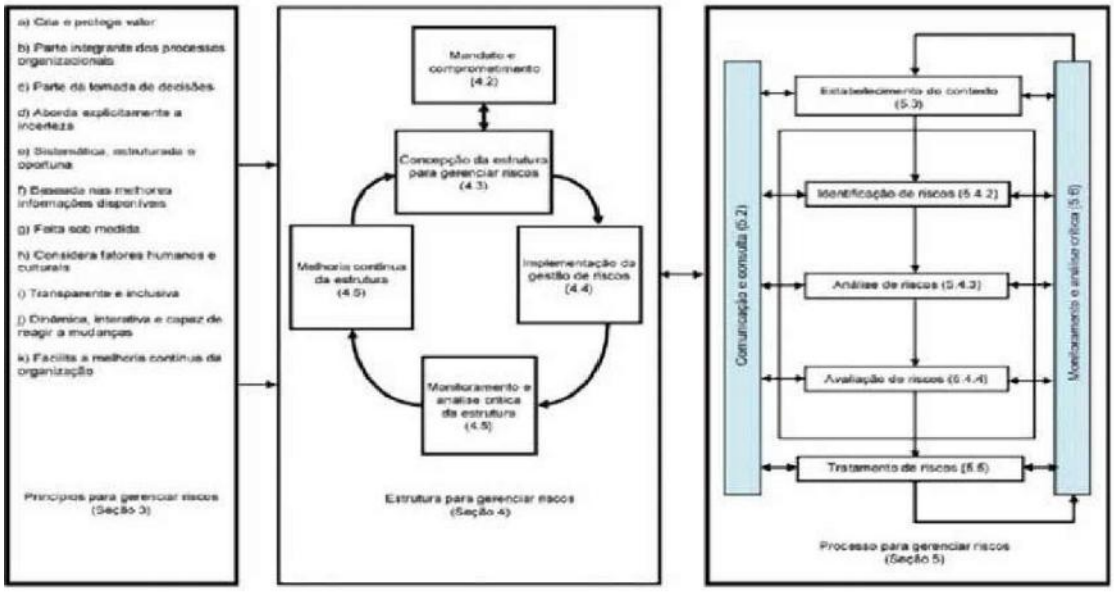
Ela não amarra uma estrutura de forma definitiva, pelo contrário, ela deixa a possibilidade de que a estrutura proposta seja adequada à realidade de cada empresa.

Dessa forma, fica claro que a ISO 31000 leva em consideração o cenário em que cada organização está inserida, o contexto tem uma importância singular em todo o processo.

É extremamente importante contextualizar a empresa antes de estruturar a gestão de risco. Não é uma receita de bolo, ela precisa ser adaptada a realidade, ao negócio da empresa que está implantando o processo.

A estrutura da ISO 31000 traz muitas novidades, dependendo da metodologia empregada pelo gestor, mas poderá ajustar aos princípios e diretrizes sem muitas dificuldades.

**A estrutura apresentada pela ABNT NBR ISO 31000/2009**




Basicamente, para tentar resumir a estrutura, ela contextualiza o negócio ou a situação da empresa e isso pode ser trabalhado através de métodos de elaboração de cenários prospectivos.

A norma não apresenta uma metodologia específica a ser utilizada.

Determinado estes contextos ou os cenários mais prováveis, são identificados quais os riscos reais ou potenciais que serão analisados.

A estrutura apresentada pela ABNT NBR ISO 31000/2009 A análise de risco busca a probabilidade e as consequências dos riscos analisados, sejam eles quantitativos, qualitativos ou mistos.

A norma não especifica quais os métodos poderão ser utilizados, além disso, o resultado da análise pode ser positivo ou negativo.

Com o resultado é realizada a avaliação dos riscos, que é a comparação do nível do risco com o apetite da empresa, por exemplo, avaliando se o risco é tolerável ou necessita de tratamento.

Essa avaliação pode ser feita através de uma ferramenta muito conhecida dos gestores, a matriz de vulnerabilidade ou de suportabilidade.

Essa matriz auxiliará o gestor na tomada de decisão, e assim fará o tratamento dos riscos, que pode ser:

1) a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;

2) tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade;

3) a remoção da fonte de risco;

4) a alteração da probabilidade;

5) a alteração das consequências;

6) o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco; e

7) a retenção do risco por uma escolha consciente.

Todo o processo apresentado envolve a comunicação e consulta dos processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos.

Além da necessidade de monitoramento e análise crítica, que pode ser aplicada, neste caso, a ferramenta bastante conhecida pelos gestores que é o PDCA.

Este monitoramento pode ser aplicado à estrutura ou ao processo de análise de risco.

No próximo mês vamos falar um pouco mais sobre a ISO 31000 e apresentar maiores detalhes sobre essa estrutura de gestão de risco.


## GESTÃO DE RISCO, A NOVA NORMA DA ABNT

No mundo empresarial contemporâneo, as empresas estão inseridas num mundo cada vez mais competitivo e uma das fontes para a manutenção da competição entre as empresas é a gestão de custos. É neste contexto que a segurança empresarial está inserida e que deve auxiliar a organização no controle desses custos.

A gestão de riscos vem ao encontro desta necessidade, aplicando, de forma estruturada, seguindo um processo da avaliação dos riscos e implementando o tratamento adequado.

Para nos auxiliar nesta missão, em 2009, foi publicada a NBR ISO 31000, que trata da gestão de riscos, a qual foi atualizada em 2018.

Agora, em 2012, foi publicada pela ABNT a NBR ISO 31010, que é uma norma de apoio à ABNT NBR ISO 31000 e fornecerá orientações para a seleção e aplicação de técnicas sistemáticas para o processo de avaliação dos riscos identificados na organização.

Assim como a NBR ISO 31000, a 31010 não é usada para fins de certificação ou uso regulatório, mas nos trará maior embasamento para sua utilização na empresa.

A NBR ISO 31010 traz diversas técnicas para a avaliação dos riscos, porém elas não se esgotam na norma.

A própria norma traz a informação de que as metodologias que não estão relacionadas, não querem dizer que não serão validas, pelo contrário, elas devem atender as necessidades da organização onde está sendo aplicada.

Assim como a 31000, a 31010 não é especifica para a segurança. Ela pode ser utilizada em qualquer segmento, sendo absolutamente genérica.

Devemos nos lembrar de que o risco não deve ser entendido apenas como uma ameaça, mas também com uma oportunidade.

Peter L. Bernstein em seu livro Desafio aos Deuses – A fascinante História do Risco escreve:

“Quando investidores compram ações, cirurgiões realizam operações, engenheiros projetam pontes, empresários abrem seus negócios e políticos concorrem a cargos eletivos, o risco é um parceiro inevitável. Contudo, suas ações revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e oportunidade”.

A NBR ISO 31010 prevê que:

O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades. Isto proporciona uma entrada para decisões sobre:

• se convém que uma atividade seja realizada;

• como maximizar oportunidades;

• se os riscos necessitam ser tratados;

• a escolha entre opções com diferentes riscos;

• a priorização das opções de tratamento de riscos;

• a seleção mais apropriada de estratégias de tratamento de riscos que trará riscos adversos a um nível tolerável. (NBR 31010)

A avaliação do risco possui em seu processo, as fases de:

Identificação dos riscos; Análise dos riscos e a própria avaliação dos riscos.

Para entender melhor, a identificação dos riscos visa, como o próprio nome diz a identificação dos riscos que podem afetar a produção, concorrência, reputação, etc. da empresa (no caso da segurança).

A análise de risco tem o objetivo de identificar, através de técnicas específicas, que pode ser qualitativa, quantitativa ou semiquantitativa para estimar a probabilidade de concretização do risco e seu impacto (perda), ainda especificamente para a segurança.

Já a avaliação dos riscos compara, normalmente através de uma matriz, o "apetite ao risco" da empresa. Isto ocorre quando ela define as ações a serem tomadas de acordo com o posicionamento dos riscos (em relação à probabilidade X impacto).

A NBR ISO 31010 apresenta uma tabela com as ferramentas mais adequadas para cada fase do processo (sem se limitar a ela), mas não é um manual para a elaboração da avaliação dos riscos.

De qualquer forma, ela é uma colaboração técnica para o nosso segmento.

## QUAL A IMPORTÂNCIA DA GESTÃO DE RISCO NO PLANEJAMENTO DA SEGURANÇA

Sempre que alguém começa a trabalhar na elaboração de um plano de segurança, o início deste planejamento deve ser a gestão de riscos.

Isso porque a gestão de riscos, alinhada a ISO 31000 impõe determinadas ações que serão essenciais à elaboração do plano de segurança.

A gestão de risco propõe um framework, ou seja, uma estrutura de processo que começa pela necessidade de se entender o contexto, o tipo de negócio da empresa analisada. Seus concorrentes, sua cultura organizacional, etc.

Esse entendimento é essencial para propor identificar os riscos e as ameaças. Muitas soluções, ainda que tecnicamente estejam corretas, podem não funcionar para determinado público, daí a importância de conhecer a cultura organizacional da empresa.

Na sequência do framework, vem a fase de identificação dos riscos. É importante fazer a ligação entre os riscos relacionados diretamente aos Fatores

Críticos de Sucesso – FCS da empresa, com o objetivo de identificar os riscos que afetam o negócio da empresa.

Na sequência será realizada a análise dos riscos identificados a fim de identificar quais as probabilidades e os impactos que eles podem trazer para a empresa, caso eles se concretizem.

Na outra fase, a avaliação dos riscos, ela mostra como os riscos relacionados e analisados serão enfrentados pela empresa. Aqueles que merecem atenção imediata, monitoramento, etc. estes riscos devem ser representados através de uma matriz de risco, que auxiliará na tomada de decisão sobre a forma de atuar em cada risco.

O tratamento dos riscos, que é a fase seguinte, identificará quais as ações necessárias para mitigar estes riscos, além de monitorar seus resultados.

Existem ainda outras duas fases que passam por todas as outras, desde o início. São as fases de comunicação e consulta e de monitoramento. Nelas, de acordo com a ISO 31000, os clientes, fornecedores e funcionários devem participar de todas as etapas listadas anteriormente.

É depois dessa análise que o plano de segurança será elaborado, pois agora você terá os riscos que devem ser tratados, as formas para mitigá-los e como monitorá-los também.

Sem este processo, o que pode ocorrer é que você esteja trabalhando com riscos que não são críticos para a empresa, dando tratamento igualitário a riscos com probabilidades e impactos diferentes, não está identificando as fontes dos riscos e demonstrará falta de estruturação no seu processo, além de não estar seguindo uma norma que foi estudada, baseada em experiência mundial, preparada e utilizada em mais de 180 países.

O plano de segurança deve ser um investimento, com retorno financeiro, deve ser mensurável, seja de maneira quantitativa ou qualitativa, mas deve medido.

Na verdade, sem isso, provavelmente você estará dando um CHUTE e criando um plano de (in) segurança que pode não atender as necessidades da empresa.

## A IMPORTÂNCIA DA GESTÃO DE RISCO NO TRANSPORTE DE CARGAS

Quando falamos em gerenciamento de riscos podemos observar a importância que ele tem em todo o processo logístico, mas especialmente no transporte de cargas.

O foco no transporte não é à toa, acontece que cerca de 60% dos custos da logística está no transporte.

O foco também é no transporte terrestre devido ao fato de 96% dos passageiros e 60% das cargas serem transportadas por este meio. Estes dados nos mostra a importância deste meio de transporte.

Para termos uma ideia dos prejuízos causados por roubo de cargas o Brasil perdeu em 2009 quase R$ 1 bilhão com roubos de cargas. De acordo com a Associação Nacional do Transporte de Cargas e Logística (NTC & Logística).

Em 2009 foram 13.500 ocorrências, sendo que cerca 80% ocorrem na região sudeste.

Neste ano, a média mensal no primeiro semestre foi de R$ 22,8 milhões só no estado de São Paulo.

Atualização - O número de roubos de carga nas rodovias federais diminuiu cerca de 35% em 2019. Segundo dados da Polícia Rodoviária Federal (PRF), foram 1.390 ocorrências no ano passado, ante 2.120 em 2018. A expectativa do setor é que a queda nos índices se consolide em 2020. https://setcesp.org.br/noticias/roubo-de-cargas-recuou-35-em-2019-nas-estradas-federais-aponta-prf/. Acesso em 06/07/20.

Estes dados ainda não contam, certamente, com os roubos não notificados, além das fraudes no desvio de estoque e roubos aos CD – centro de distribuições.

O gerenciamento de riscos deve ser estruturado, de acordo com a ISO 31000, que apresenta em seu framework todos os processos para a estruturação da gestão de riscos.

Além disso, o custo da perda não está apenas no valor do material roubado e sim em todo o transtorno causado pelo roubo de uma carga. Veja os prejuízos que trazem se utilizarmos a formula do Custo da Perda, que é:

CP= Sp + St + Cc + Rc – (I-P)

**SP –** é a substituição permanente do produto, aquilo que foi efetivamente roubado.

**ST –** é a substituição temporária, ou seja, os recursos gastos com a operacionalização de substituir temporariamente o caminhão, motoristas, pedágios, frete, e tudo que foi gasto para atender a ocorrência.

**CC -** é o custo consequente, que é a perda gerada em decorrência da ocorrência, que pode ser, em muitos casos, maior do que o valor da carga, como por exemplo a perda de um cliente.

**Rc –** é a redução do dinheiro em caixa, que neste caso só será contabilizado o dinheiro, em espécie, caso tenha sido roubado ou se também era transportado.

**I –** é a indenização que o seguro pagará, caso a carga esteja segurada.

**P –** é o prêmio pago ao seguro até o momento da ocorrência e sabemos que o valor é maior devido ao tipo de carga e a quantidade de ocorrências existente.

Com esta pequena fórmula do Custo da Perda, já é possível mensurar, pelo menos de uma maneira mais aproximada, a perda financeira numa ocorrência de roubo de carga.

Esse valor nos ajuda a tomarmos medidas para mitigar a probabilidade e/ou a perda dos roubos de cargas.

É aí que entra a gestão de risco com toda a sua estrutura que, necessariamente não é apenas em escolta ou sistema de rastreamento.

A identificação dos fatores de risco, ou seja, as causas para que o risco de roubo de cargas aconteça leva em consideração diversos fatores, que vão desde a escolha dos funcionários, análises das ocorrências, trajeto a ser percorrido, locais de parada, etc.

Apesar de a ISO 31000 não apresentar os métodos que devem ser utilizados para a identificação dos riscos, análise de riscos, avaliação dos riscos e monitoramento (que serão apresentadas na ISO 31010, ainda sem tradução para o português) + (publicada no Brasil em 04/04/2012) ela nos dá a estrutura da gestão e apresenta os processos que o gestor de riscos deve seguir, utilizando as ferramentas que ele já utilizada hoje, pois nenhuma delas foi invalidada.

Devemos lembrar que o objetivo logístico, é ter o produto certo, na quantidade certa, na hora certa, no lugar certo ao menor custo possível.

Os custos das perdas na logística traz impacto para toda a sociedade e não apenas para as transportadoras, pois estas perdas são repassadas, de uma forma ou de outra, para os consumidores, que somos todos nós.

A ISO 31000 veio para ficar e deve ser adaptada à realidade de cada empresa, e esta pode manter a sua metodologia, suas ferramentas, porém, convém que ela comece a se estruturar conforme a indicação da norma na busca de uma diminuição das perdas.

# GESTÃO DE RISCO - IDENTIFICAÇÃO DOS RISCOS E FATORES DE RISCO

**Identificação dos riscos:**

Aqui, vamos procurar identificar os riscos que a empresa, condomínio, agência bancária, ou seja lá o que estiver sendo analisado, estão sujeitos. Lembrando que risco é o efeito da incerteza nos objetivos (**ABNT NBR ISSO 31000:2018)** e, quando identificamos um risco, estamos identificando um efeito e, portanto, haverá necessidade de identificarmos as causas para que este efeito ocorra. Então, podemos citar como exemplos de riscos: incêndio, roubo, sequestro, desvio interno, fuga de informação, etc.

Antes de falarmos sobre os métodos, é preciso ter a clara ideia de que não existe um método ruim, as pessoas se adaptam melhor a determinados métodos, assim como as circunstâncias também podem nos levar a adotar um método específico.

Um destes métodos para identificação do risco é o **B*rainsntorm*** (tempestade de ideias), pois é um dos mais utilizados.

Ele foi criado em 1938 por **Alex Osborn**, que afirma: "*uma pessoa normal consegue criar duas vezes mais ideias em grupo do que individualmente*",

portanto a primeira regra que observamos é que este método é realizado por um grupo de pessoas.

Por que usaríamos um grupo de pessoas para identificar os riscos da empresa? Porque com um grupo de pessoas podemos ver todos os ângulos da empresa. Seria injusto imaginar que o gestor de segurança ou quem estiver fazendo a análise de risco, tivesse obrigação de conhecer todos os processos, que podem ser inúmeros em uma determinada empresa, e pudesse identificar todos os riscos que a empresa está exposta. Daí a necessidade da participação de pessoas das diversas áreas. Normalmente as áreas participantes são: recursos humanos, marketing, financeiro, produção e segurança, dependendo do tipo de negócio.

Ele consiste em expor uma situação e as pessoas vão falando, de uma maneira ordenada, aquilo que elas percebem, ou seja, os riscos existentes naquele processo. *"Processo é um conjunto de atividades logicamente inter-relacionadas, envolvendo pessoas, equipamentos, procedimentos e informações que, quando executadas, agregam valor e produzem resultados específicos".*

Um detalhe importante é que não deve haver críticas sobre as ideias que surgem e que serão analisadas posteriormente.

Deve haver uma pessoa no comando deste processo, todas as ideias devem ser relacionadas e esta reunião não deve ultrapassar uma hora de duração sob pena de perder o seu objetivo.

Em resumo:

Não pode ser conduzido por pessoas que não estejam familiarizadas com os processos da empresa; requer a participação ativa de todos, ninguém deve ter medo de expor, inexiste hierarquia e defesas do lado de fora; não existem ideias ruins; não existem perguntas bobas; tudo deve ser anotado para posterior avaliação.

Além deste método que é usado, principalmente, para riscos potenciais, devemos usar o histórico da empresa.

Quais foram os riscos que, de fato, se concretizaram no site analisado? Para isso, uma das formas mais utilizadas é a entrevistas com as pessoas

envolvidas em cada processo crítico da empresa, por isso a importância de se trabalhar com as pessoas que conhecem a empresa.

Nestas entrevistas vamos procurar os históricos de ocorrências na empresa e/ou em empresas similares. Outro fator importante é saber como as empresas que têm o mesmo atrativo estão fazendo para gerenciá-los, ou seja, quais são os modelos adotados pelo mercado (você pode adaptá-los para sua empresa).

Levantar quais foram as perdas internas, daí a importância de um banco de dados estruturado.

Outra forma é a do ***Benchmarking***, que é a busca pelas melhores práticas que conduzem uma empresa à maximização da performance empresarial.

A **Xerox Corporation** foi pioneira na utilização do *Benchmarking*, onde teve sua definição como sendo um processo contínuo de medição de produtos, serviços e práticas em relação aos mais fortes concorrentes, ou às empresas reconhecidas como líderes em suas indústrias

O *benchmarking* pode ser tanto uma descrição do estado atual das operações da empresa quanto uma descrição das melhores práticas tidas como objetivos da empresa.

Através da análise dos processos que a empresa desenvolve é possível identificarmos quais são os processos críticos, aqueles que têm maior influência no resultado da empresa, com isso identificamos os maiores riscos aos quais a empresa está sujeita.

A colaboração que o *benchmarking* traz para a análise de risco é no conhecimento dos processos da empresa e, através dele, conseguimos identificar os riscos reais e potenciais. Também é importante que sempre levemos em consideração o ambiente interno e externo.

Seja qual for o método utilizado para a identificação dos riscos será importante saber por que eles ocorrem, quais suas causas, ou seja, buscar suas origens.

Encontrar as causas que influenciam na concretização do risco é fundamental pois será baseado nestes fatores de risco, que o gestor poderá traçar seu plano de ação.

Veja que os fatores de risco, são as origens de cada risco e que serão, baseados nos fatores de risco relacionados, que as ações devem ser implementadas.

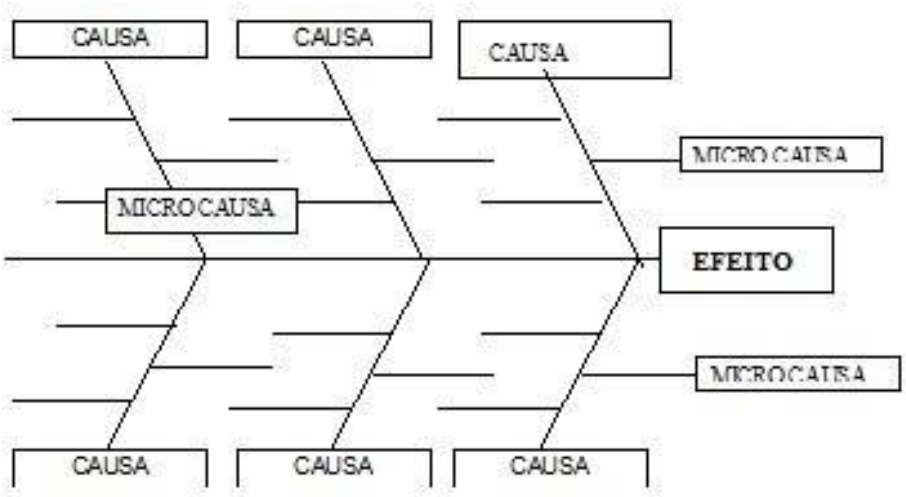
Quando elaboramos nossos planos de ação, ele deve ser baseado nas causas e não nos efeitos (riscos), desse modo fica claro que nossas ações serão, de maneira direta, sobre os fatores relacionados. Daí a importância de elaborar, de forma consistente, estes fatores.

O método mais comum usado pelos gestores é o de diagrama espinha de peixe, também chamado de diagrama de causa e efeito ou ainda de diagrama de Ishikawa, em homenagem ao engenheiro japonês, **Kaoru Ishikawa**, que utilizou esse diagrama pela primeira vez em 1943.

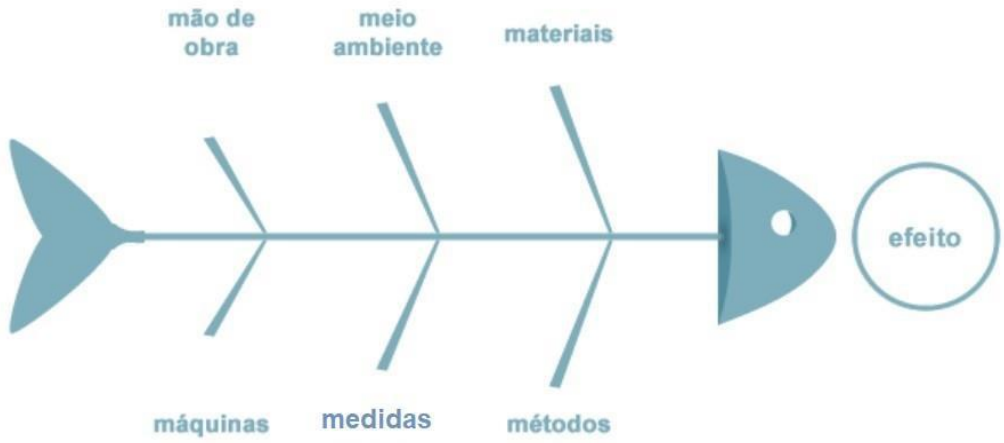
O diagrama se parece com uma espinha de peixe e busca as causas de um determinado efeito.

Este processo, além de ser muito eficaz é muito simples e fácil de usar.

Consiste em, a partir da identificação de um efeito indesejável, no nosso caso, o risco e começarmos a fazer a pergunta por que? E por que? Até estratificarmos todos os possíveis fatores.




No processo de qualidade ele foi usado como 6M, onde cada M se referia a uma das espinhas do peixe e eram relacionados os fatores de risco (causas) para cada uma delas. Os “Ms” eram: Medidas, Meio Ambiente, Mão-de-obra, Materiais, Métodos e Máquinas.

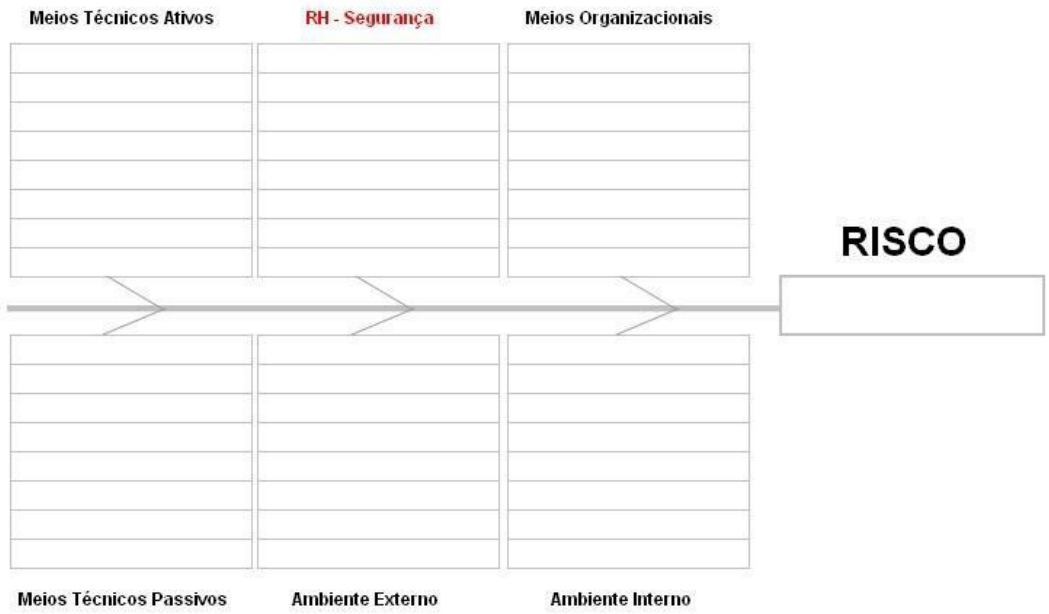



Para o processo de análise de risco podemos usar quaisquer outras categorias, como por exemplo: pessoas, equipamentos, etc.

No método **Brasiliano** de análise de risco foram sugeridas as seguintes categorias: Recursos Humanos da Segurança; Meios Organizacionais; Meios Técnicos Ativos; Meios Técnicos Passivos, Ambiente Interno e ambiente Externo.

Sejam quais forem as categorias escolhidas, devem ser dissecadas até a origem de cada uma delas, de acordo com a sua aplicabilidade.

O diagrama fica assim definido:




O diagrama estabelece a relação entre o efeito e suas causas e possibilita um detalhamento das causas, facilitando a elaboração do plano de ação. Também

permite que o usuário explore as várias categorias das causas e incentiva a criatividade através de um processo de *Brainstorming*.

**A árvore de falhas** é também uma das ferramentas que podemos usar. A análise de Árvore de Falhas - AAF foi primeiramente elaborada por **H.A.Watson** dos Laboratórios Bell Telephone em 1961, a pedido da Força Aérea Americana para avaliação do sistema de controle do *Míssil Balístico Minuteman*.

A árvore de falhas é um método para o estudo dos fatores que poderiam causar um evento indesejável (falha) e encontra sua melhor aplicação no estudo de situações complexas. Ela determina as frequências de eventos indesejáveis (topo) a partir da combinação lógica das falhas dos diversos componentes do sistema.

No contexto de riscos operacionais, a árvore de falha classifica os eventos que conduzem ao principal, tais como pessoal, procedimento ou de equipamento.

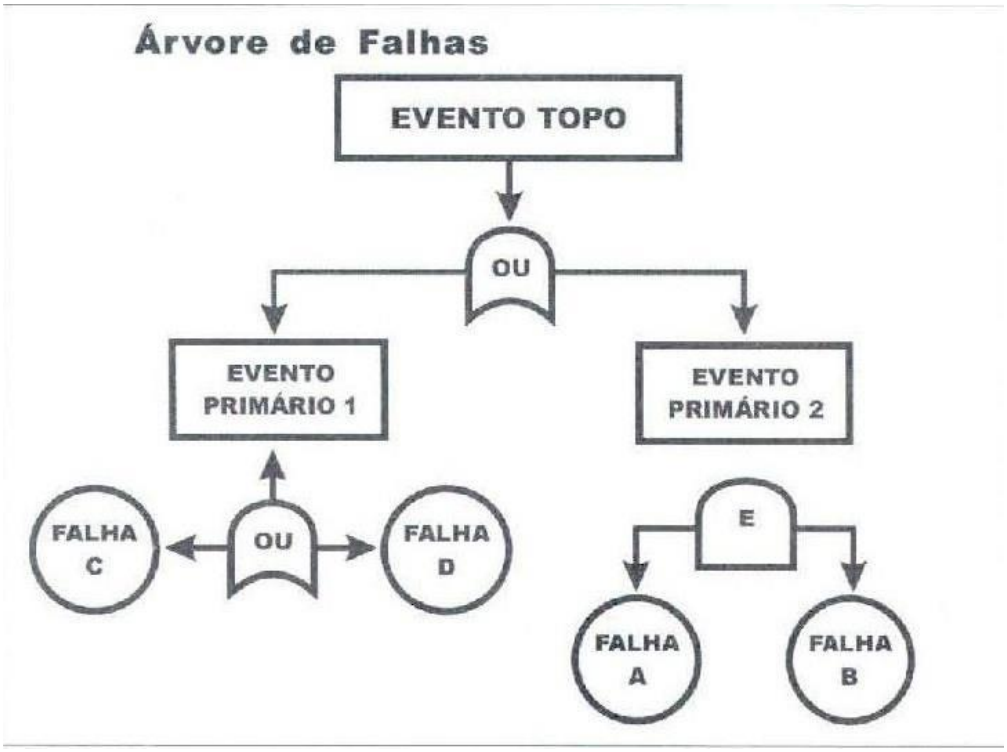
O evento indesejado recebe o nome de evento topo por uma razão bem lógica, já que na montagem da árvore de falhas o mesmo é colocado no nível mais alto. A partir deste nível o sistema é dissecado de cima para baixo, enumerando todas as causas ou combinações delas que levam ao evento indesejado. Os eventos do nível inferior recebem o nome de eventos básicos, primários ou ainda de "filhotes", pois são eles que dão origem a todos os eventos de nível mais alto.

O processo de construção da árvore tem início com a percepção ou previsão de uma falha, que a seguir é decomposto e detalhado até eventos mais simples Os eventos primários, aqueles que dão origem aos outros eventos, precisam ser tratados da mesma forma, qual seja, de cima para baixo.

Com a adição de elementos lógicos ao diagrama, como 'E' e 'OU', melhora a caracterização dos relacionamentos entre as falhas. Dessa forma é possível utilizar o diagrama para estimar a probabilidade de uma falha acontecer a partir de eventos mais específicos.

A porta E significa que o evento principal ocorre se todos os eventos primários ligados pela mesma porta ocorrerem ao mesmo tempo. Uma porta OU significa que o evento principal ocorre se qualquer um dos eventos ligados pela porta ocorrer em um dado tempo.

Veja o diagrama abaixo:




A importância da árvore da falha no processo de análise de risco é que podemos saber em termos quantitativos a probabilidade de os eventos ocorrerem ao mesmo tempo, sendo independentes ou inter-relacionados. Daí a grande importância da árvore de falha no gerenciamento de riscos corporativos. O evento principal só ocorrerá quando todos os eventos primários ocorrerem simultaneamente.

As árvores de falha são mais adequadas para análise das causas de um evento conhecido em particular envolvendo um risco crítico.

As árvores de falha não representam a passagem do tempo, sendo mais adequadas para eventos essencialmente aleatórios. Elas ainda oferecem uma abordagem extremamente flexível incorporando soluções quantitativas e qualitativas ou baseadas em simulações.

Os métodos que foram apresentados, ainda que superficialmente, não esgotam, de forma alguma, a quantidade de ferramentas que o gestor poderá utilizar na identificação dos riscos e seus fatores de riscos.

Lembro que a identificação dos fatores de riscos é de extrema importância pois serão utilizados para a elaboração do plano de ação. O plano de ação deve atuar nas causas e não no efeito.


## DIAGNÓSTICO DE SEGURANÇA

Diagnóstico de segurança é um conceito bastante disseminado na segurança empresarial.

A segurança empresarial traz diversos conceitos de outras disciplinas, como a administração, Marketing e qualidade, por exemplo, sendo neste caso, a disciplina de administração formulou o conceito de diagnóstico, sendo adaptada para a segurança como diagnóstico de segurança.

Aqui vou apresentar, de maneira resumida, uma das formas de se realizar o diagnóstico de segurança, mas antes vamos identificar a origem desse conceito.

De acordo com Idalberto Chiavenato, em seu livro, **Administração nos Novos Tempos** (1999), apesar de já haver registros escritos de atividades comerciais e governamentais ao redor do ano de 5.000 a.C., foi só a partir do século XVIII, com a Revolução Industrial, a qual alterou a configuração mundial, transferindo o centro de negócios da agricultura para a indústria.

Mas a teoria da administração só teve início em 1903 com o primeiro livro de **Frederick Winslow Taylor,** "Shop Management" (Direção de Oficinas) onde trata pela primeira vez de suas ideias sobre a racionalização do trabalho. Tem início a administração cientifica.

Depois houve muitas mudanças e a evolução conceitual, inclusive a de diagnóstico.

Para o professor e pesquisador Antonio Francisco Domingues Loriggio, o conceito de diagnóstico é universal e que fundamentos válidos para determinada ciência podem ser também válidos ou estendidos para a Administração. Um desses temas está associado ao estudo e à aplicação de *expert systems* ou sistemas especialistas. Muitas aplicações de tais sistemas têm sido voltadas para o auxílio ao diagnóstico de problemas tanto em Medicina quanto em Eletrônica. Matéria publicada no **caderno de pesquisas em administração (1996).**

Chiavenato em outro livro, **Introdução à teoria geral da administração: uma visão abrangente da moderna administração das organizações** (2004), conceitua diagnóstico organizacional como, a partir da análise dos dados colhidos, passa-se a sua interpretação e diagnóstico: procura-se identificar preocupações e problemas, suas consequências, estabelecer prioridades e estabelecer os alvos e objetivos.

A finalidade do diagnóstico organizacional é o estabelecimento de uma compreensão amplamente partilhada e de um sistema baseado nessa compreensão para determinar se a mudança é desejável.

Desse modo, seguindo a linha da administração e seus conceitos sobre diagnóstico, surge o conceito de diagnóstico de segurança, já bastante difundido.

O professor Dr. Antonio Celso Ribeiro Brasiliano, em seu livro **Inteligência em Risco** (2016) conceitua diagnóstico como um processo de conhecer as condições que deve responder a pergunta básica: “Qual a situação real da empresa, processos e ou departamentos quanto aos seus aspectos de controle e segurança, frente à sua política de gestão de riscos e aos seus objetivos estratégicos? ” Essa análise deve ser efetuada da forma mais realista possível, pois qualquer distorção prejudicará todo o resto do processo de desenvolvimento e implantação de medidas preventivas e mitigatórias.

A **Núcleo Consultoria**, define que o Diagnóstico de Segurança responde às perguntas: Como está a segurança? Qual plano de ação seguir para atingir o nível desejado?

Para seguirmos o processo da ISO 31000, **Gestão de riscos — Diretrizes,** publicada em 2018, devemos acompanhar sua estrutura.

Ela começa com a contextualização, a ISO Guia 73/2009 **Gestão de riscos – Vocabulário** e conceitua como estabelecimento do contexto, a definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos.

Entram aqui, o contexto externo, que é o ambiente externo no qual a organização busca atingir seus objetivos e o contexto interno, que é o ambiente interno da organização.

O **contexto externo** pode incluir: o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local; os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e as relações com **partes interessadas (***Stakeholders)* externas e suas percepções e valores.

Ainda de acordo com o GUIA ISO 73, o **contexto interno** pode incluir: governança, estrutura organizacional, funções e responsabilidades; políticas, objetivos e estratégias implementadas para atingi-los; capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias); sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais); relações com partes interessadas internas, e suas percepções e

valores; cultura da organização; normas, diretrizes e modelos adotados pela organização; e forma e extensão das relações contratuais.

Na sequência da estrutura da ISO 31000, vem a Identificação dos Riscos. Nesse caso, uma das ferramentas que pode ser utilizada é o Brainstorming, que é uma técnica indicada pela ISO 31010 **Gestão de riscos — Técnicas para o processo de avaliação de riscos**, publicada em 2012.

Através desta ferramenta será possível identificar os riscos da organização.

Depois de identificado os riscos, devemos identificar as causas de cada risco, até porque devemos combater as causas e não seus efeitos.

Para isso podemos utilizar a ferramenta do diagrama de causa e efeito, também conhecido como Ishikawa, devido ao nome do seu criador.

Nesse caso, mais uma vez adaptando de outra disciplina (Qualidade), ao invés de usarmos os 6 Ms, como foi desenvolvido por Kaoru Ishikawa, (Método, Máquina, Medida, Meio Ambiente, Mão-de-Obra, Material), usaremos os macros causas como RH da Segurança; Meios Organizacionais; Ambiente Externo; Ambiente Interno; Meios Técnicos Ativos e Meios Técnicos Passivos.

Assim como foi adaptado dos 6 M, estes macros causas também podem ser adaptadas de acordo com a organização.

No livro citado do professor Brasiliano, ele utiliza os macros causas como: Processos; Pessoal; Infraestrutura; Tecnologia e Ambiente Externo. Portanto cinco macros causas.

Esta ferramenta é muito importante e quando bem elaborada, tem um formato de espinha de peixe e identifica todos os fatores de risco, ou seja, porque cada risco pode ocorrer, sendo este método também citado na ISO 31010/2012.

Ainda na fase de identificação de riscos, podemos sintetizar todo o trabalho através de uma matriz.

A SWOT é um acrônimo das palavras Strenghts, Weaknesses, Opportunities e Threats, também conhecido como FOFA - Forças, Oportunidades, Fraquezas e Ameaças.

De acordo com Henry Mintzberg, no livro **Ascenção e Queda do Planejamento Estratégico** (2004), foram dois professores da Harvad Business School que formalizaram este conceito, Kenneth Andrews e Roland Cristensen.

A matriz SWOT estuda a competitividade de uma organização segundo suas quatro variáveis.

Seu objetivo é mostrar a situação da empresa naquele momento, por isso é também conhecida como uma fotografia da empresa.

De acordo com a metodologia apresentada aqui, nós conseguiremos preencher apenas parte da Matriz SWOT.

Nós teremos identificado através dos diagramas de causa e efeito, (lembrando que é um diagrama para cada risco identificado) as fraquezas e as ameaças e não as forças e oportunidades.

As fraquezas são todos os fatores de riscos identificados nos diagramas, exceto o de ambiente externo, estes serão incluídos no quadrante das ameaças.

As oportunidades (que são positivas) e as ameaças (que são negativas) são consideradas como variáveis incontroláveis, pois não estão nas mãos da empresa para controla-las.

Por exemplo, se foi identificada como fator de risco a criminalidade no entorno da empresa ou o crime organizado, isso não está nas mãos da empresa para que ela possa controlar. Ela poderá influenciar, mas não decide sobre esses fatores.

Já nas fraquezas, relacionadas no diagrama de causa e efeito, como por exemplo, a falta de iluminação, a falta de procedimentos, de câmeras, etc. são fatores que dependem apenas da empresa para implementá-los.

No caso das forças, são os fatores positivos que a organização já possui, como por exemplo, equipe de vigilantes, câmeras, políticas, etc.

Então, as forças (interna) e oportunidades (externa) são fatores positivos e as fraquezas (internas) e as ameaças (externas) são fatores negativos.

Desse modo, através da Matriz SWOT se tem uma visão, um diagnóstico de segurança da empresa.

Além disso, é possível identificar os fatores mais motrizes, aqueles que alavancam outros fatores, que devem ser os primeiros a serem tratados.

Para isso, Brasiliano identifica sua Magnitude e Importância da seguinte forma:

**Magnitude** significa o tamanho ou grandeza que a variável ou evento possui perante o contexto empresarial. Caso aconteça, positiva ou negativamente, o quanto ela vai influenciar no contexto como um todo.

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).

Como parâmetro para avaliar a magnitude nas células de fraqueza e ameaça, é levado em consideração o número de vezes que as variáveis aparecem no diagrama de causa e efeito.

**Importância** significa a prioridade que essa variável deve possuir perante o contexto do empresarial. É uma nota subjetiva com base na experiência do gestor e da equipe que está avaliando o cenário. Para análise da importância, utilizamos 3 níveis de pontuação:

3 (muita importância);

2 (média importância);

1 (pouca importância).

Para criar um ranking dos itens em cada célula da Matriz, multiplicamos a avaliação da magnitude e da importância.

Os fatores de riscos com maior pontuação negativa são considerados motrizes, pois podem influenciar diretamente os riscos identificados.

A diferença entre o diagrama de causa e efeito e a SWOT é que o diagrama “enxerga” apenas as causas de um determinado risco, enquanto que a SWOT “vê” o todo e classifica as prioridades.

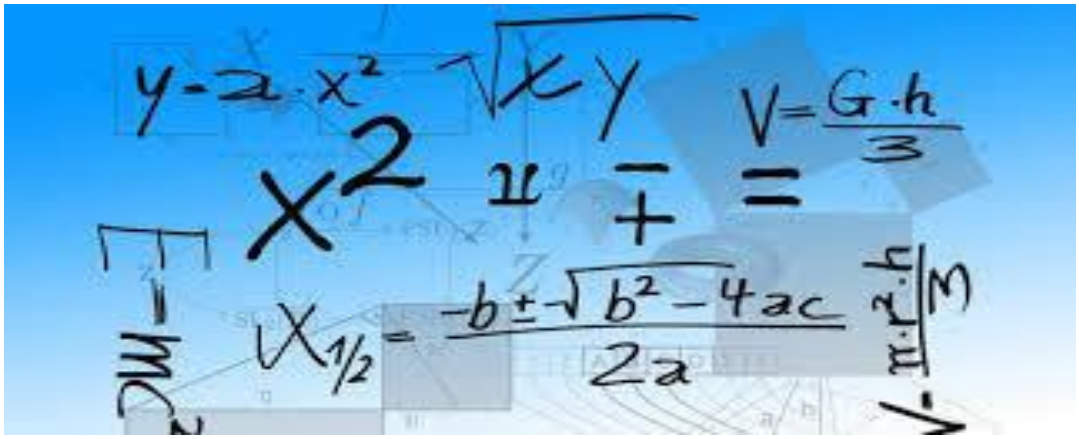
Dessa forma, o gestor poderá tomar decisões baseadas em técnicas experimentadas e que acompanham as normas de gestão de risco.

A aplicação desta metodologia é simples, porém trabalhosa, mas que trará uma visão mais sistêmica ao diagnóstico de segurança.

A matriz SWOT apresenta, de forma clara, a situação daquele momento da empresa, apresentando as oportunidades de melhoria no sistema de segurança empresarial.

Outro fator importante é que, de acordo com a ISO 31000 a Comunicação e Consulta, além do Monitoramento e Análise Crítica, serão partes integrantes de todas as fases, o que demonstra a importância da participação das pessoas nas fases do processo de gestão de riscos.

Lembramos que esta é apenas uma das possibilidades para se realizar o diagnóstico, existem outras mais simples ou mais complexas, caberá a cada um usar e adaptar as ferramentas de acordo com os seus objetivos.




## METODOLOGIA PARA ANÁLISE DE RISCOS – MÉTODO ESTATÍSTICO (ATUALIZADO)

Se compararmos com outros segmentos, o mercado de segurança empresarial ainda é muito recente, tanto que há poucos métodos e teorias para suportar a prestação deste tipo de serviço. Normalmente, decide-se o quanto investir em um determinado projeto de maneira empírica, ou seja, sem base técnica, usando apenas a experiência, que é fundamental, mas nem sempre será suficiente.

Por que devemos fazer a análise de riscos e o que buscamos com estas metodologias?

Ao fazer uma análise de riscos, buscamos respostas para duas perguntas básicas:

1). Qual a probabilidade de um determinado risco ocorrer?

2). Qual o impacto tangível ou intangível que esse risco terá sobre o negócio?

Quando falamos de risco (futuro), podemos trabalhar com metodologias, que apesar de serem usadas pelo pessoal da segurança, devem ter a participação de outras pessoas da empresa para que possam mensurar os valores e as probabilidades.

Não existe a possibilidade de o gestor de segurança ou consultor de segurança realizar a avaliação de risco sozinho, sem a participação de quem conhece a empresa.

Quando conseguirmos mensurar esses valores e percentuais, poderemos multiplicá-los e encontrar o valor máximo a ser investido para aquele determinado risco.

Este valor é chamado de PERDA ESPERADA porque se nada for feito e o cenário não for alterado, esse é o valor que a empresa poderá perder. Em suma, não podemos gastar mais do que o que a empresa perderia se não fizesse nada.

Um exemplo: Imagine que você, após a análise de risco, tenha chegado à conclusão de que há uma probabilidade de 75% de ocorrer um incêndio em sua empresa e que, se isso acontecer, a perda (em imagem, produtos, dias parados, equipamentos novos e de substituição temporária etc.) será de R$ 350 mil.

Nesse caso, o valor da perda esperada será de R$ 262.500 (R$ 350 mil x 75%). Logo, o valor máximo a ser investido em um projeto de prevenção e combate a incêndio será de R$ 262.500.

O mesmo exemplo pode ser utilizado para casos de furto, desvio interno, roubo de carga, entre outras ocorrências.

Nem sempre os valores da perda serão fáceis de identificar, em muitos casos os valores recebem uma classificação, como por exemplo: o impacto é insignificante, leve, moderado, severo ou massivo.

Lembrando que quem determina o impacto é a empresa e não o gestor ou consultor. É a direção da empresa que identifica o valor ou mensura essa perda.

Normalmente, o empresário quer saber em quanto tempo recuperará este gasto. O papel do gestor de segurança é mostrar-lhe que a “não perda” é que irá gerar o recurso para o financiamento do projeto de segurança e a transformação do “gasto” ou custo de segurança em investimento.

Além disso, sabendo-se quanto teremos de “não perda” nos meses seguintes, podemos calcular o retorno do investimento, inclusive usando as metodologias utilizadas pela empresa.

Os métodos mais comuns utilizados para decidir sobre a aprovação de um determinado projeto são o Fluxo de Caixa, Payback, Payback descontado, o Valor Presente Líquido (VPL) e Taxa Interna de Retorno (TIR).

Podemos dividir em dois grupos as metodologias para análise de risco: métodos objetivos/quantitativos e subjetivos/qualitativos.

Os métodos objetivos, também chamados de quantitativos, são aqueles que usam dados de ocorrências passadas, ou seja, que possuem um histórico. Nesse ponto é bom ressaltar que um dos problemas que enfrentamos na segurança empresarial é a falta de banco de dados, de registros sistemáticos de ocorrências que trazem algum tipo de perda para a empresa, fato que dificulta muito a análise de risco.

Os métodos subjetivos, também chamados de qualitativos, são aqueles que partem de pouco ou nenhum histórico de ocorrências. Por exemplo, no caso de uma nova instalação ou prestação de serviço que a empresa passará a fazer, é preciso fazer a análise de risco, porém não há um histórico. Nesse caso a solução é buscar empresas similares que estejam instaladas em locais com o mesmo nível de segurança para levantar dados com o objetivo de analisar as condições de risco.

Os métodos utilizados na análise de riscos podem ser qualitativos, semiquantitativos ou quantitativos.

O grau de detalhe requerido dependerá da aplicação em particular, da disponibilidade de dados confiáveis e das necessidades de tomada de decisão da organização. (ABNT NBR 31010:2012)

Métodos objetivos

A probabilidade (P) pode ser pensada como a teoria matemática utilizada para estudar a incerteza oriunda de fenômenos que envolvem o acaso. Este método simples é indicado para casos específicos em que a probabilidade representa o número de vezes que um determinado evento pode ocorrer em uma determinada atividade, dividido pela quantidade de eventos possíveis em uma mesma atividade.

Como em todos os métodos quantitativos, será necessário possuir histórico de ocorrências.

A fórmula de cálculo é muito simples: P = N /T

Onde: P = probabilidade de um evento ocorrer; N = número de vezes que ocorre o evento e T = número total de eventos.

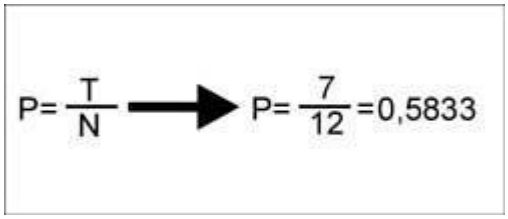
O substituto mais comum para a probabilidade de um evento frequente é o número de ocorrências do evento durante algum período de tempo: sua frequência.

Dessa forma:

N = número de ocorrências durante um período de tempo.

T = extensão do período de tempo histórico

Exemplificando: Uma agência bancária teve sete assaltos num período de doze meses, então:




Há uma probabilidade de 58,33% de chance de a agência ser assaltada a cada mês.

Método estatístico

Dos métodos objetivos, o mais utilizado pela segurança empresarial é o Estatístico, que faz uma projeção da probabilidade de o risco permanecer, caso o cenário não seja alterado. Esta metodologia se apoia em dados de fatos ocorridos e deve ser usada nas situações em que o cenário não tenha sido modificado.

Para utilização deste método, porém, o primeiro passo é possuir histórico de ocorrências, pois ele só será útil se houver registros das ocorrências a serem analisadas.

Média aritmética

A média aritmética de um conjunto de dados é a soma de todos os itens dividida pelo número deles. Na análise de riscos ela nada mais é do que a soma de todas as ocorrências de um determinado período dividida pelo período de tempo analisado. A fórmula é a seguinte:

$$\overline{X} = \frac{Xi}{n}$$

Onde: Xi = somatória das ocorrências e n = o período de tempo

Exemplificando: uma determinada carga tem o seguinte histórico de roubos:

| Ano | N° de roubos |
|---|---|
| 2001 | 06 |
| 2002 | 05 |
| 2003 | 08 |
| 2004 | 06 |
| 2005 | 05 |
| Total | 30 |

$$Xi = \frac{06+05+08+06+05}{05}$$

$$X = \frac{30}{5}$$

Nesse caso, a média de roubos desta carga é de 06 por ano.

Uma vez encontrada a média, é preciso procurar o Desvio Padrão (S) que nos mostrará o quanto a média pode variar para mais ou para menos. Logicamente, quanto maior for a diferença entre o número de ocorrências, maior será o Desvio Padrão.

A fórmula usada nesse caso é:

$$S = \sqrt{\frac{\Sigma (Xi-X)^2}{N}}$$

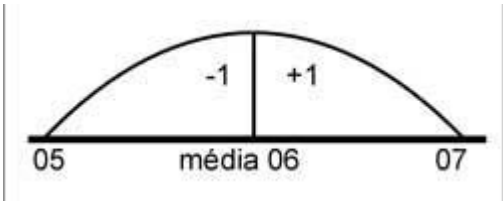
Assim, usando o exemplo anterior temos:

$$S = \sqrt{\frac{(6-6)^2+(5-6)^2+(8-6)^2+(6-6)^2+(5-6)^2}{5}}$$

$$S = \sqrt{\frac{0+1+4+0+1}{5}} = \sqrt{1,2} =$$

$$S = 1,09$$

Neste exemplo a média, que é 6, pode variar de 5 até 7 roubos por ano, ou seja, um para mais ou um para menos. Outra forma de demonstrar isso é:




Com o resultado do Desvio Padrão, é possível calcular qual o Coeficiente de Variação (CV). O Coeficiente de Variação nos dará o grau de incerteza, que é o quanto a resposta encontrada pode estar ERRADA.

A fórmula é: CV = S / X

Sendo: S= Desvio Padrão e X = Média Aritmética

Ainda usando o exemplo anterior, o resultado será:

$$CV = \frac{1,09}{6} = 0,1816$$

Assim, há 18,16% deste resultado estar errado.

Neste caso, se pegarmos a probabilidade máxima que é de 100% e tirarmos os 18,16% temos 81,84% de chance de a resposta estar CORRETA.

Ou seja, a probabilidade de que este tipo de roubo continue no próximo ano (entre 5 e 7 ocorrências), se nada for feito, é de 81,84%.

Impacto no negócio

As consequências e suas probabilidades podem ser determinadas por modelagem dos resultados de um evento ou conjunto de eventos, ou por extrapolação a partir de estudos experimentais ou a partir dos dados disponíveis.

As consequências podem ser expressas em termos de impactos tangíveis e intangíveis. Em alguns casos, é necessário mais que um valor numérico ou descritor para especificar as consequências e suas probabilidades em diferentes períodos, locais, grupos ou situações (ABNT NBR31000:2009).

Para calcular o impacto financeiro da perda do exemplo citado, não podemos calcular apenas no valor do material roubado e sim em todo o transtorno causado pelo roubo de uma carga.

A análise de consequências pode envolver: .... Considerar as consequências secundárias, tais como aquelas que impactam os sistemas, atividades, equipamentos ou organizações associadas (ABNT NBR 31010:2012).

Veja os prejuízos que trazem se utilizarmos a formula do Custo da Perda, que é:

CP= Sp + St + Cc + Rc – (I-P)

**SP –** é a substituição permanente do produto, aquilo que foi efetivamente roubado.

**ST –** é a substituição temporária, ou seja, os recursos gastos com a operacionalização de substituir temporariamente o caminhão, motoristas, pedágios, frete, e tudo que foi gasto para atender a ocorrência.

**CC -** é o custo consequente, que é a perda gerada em decorrência da ocorrência, que pode ser, em muitos casos, maior do que o valor da carga, como por exemplo a perda de um cliente.

**Rc –** é a redução do dinheiro em caixa, que neste caso só será contabilizado o dinheiro, em espécie, caso tenha sido roubado ou se também era transportado.

**I –** é a indenização que o seguro pagará, caso a carga esteja segurada.

**P –** é o prêmio pago ao seguro até o momento da ocorrência e sabemos que o valor é maior devido ao tipo de carga e a quantidade de ocorrências existente.

Com esta pequena fórmula do Custo da Perda, já é possível mensurar, pelo menos de uma maneira mais aproximada, a perda financeira numa ocorrência de roubo de carga.

Perda esperada

Com o resultado da análise de risco é possível calcular o valor da perda esperada, isto é, o quanto a empresa irá perder se não fizer nada e se o cenário atual não mudar.

Para isso, é preciso multiplicar o valor do impacto financeiro (R$) com a probabilidade (%).

Baseado no caso anterior, vamos supor que o impacto financeiro da empresa com os roubos de carga tenha sido de R$ 300 mil ao ano.

Como há uma probabilidade de 81,84% desta média se manter, temos o valor da perda esperada que é R$ 300 mil X 81,84% = R$ 245.520,00.

Caso a empresa não faça nada, terá uma perda de R$ 245.520,00 ao ano.

O valor da perda esperada também será utilizado para calcular o teto dos gastos com a segurança. Assim, não há como justificar um gasto superior do que aquele que a empresa irá perder se não fizer nada.

Em suma, é possível aplicar o método estatístico quando:

• Houver histórico de ocorrências;

• Não houver alteração do cenário;

• Quisermos uma projeção baseada em fatos já ocorridos.

Com o resultado da análise de risco encontraremos:

• A probabilidade de o risco se concretizar;

• O valor do impacto financeiro das perdas;

• O valor da perda esperada, se nada for feito;

• O valor máximo a ser investido para mitigar o risco analisado.

A análise quantitativa completa pode nem sempre ser possível ou desejável devido a informações insuficientes sobre o sistema ou atividade que está sendo analisado, à falta de dados, à influência dos fatores humanos etc., ou porque o esforço da análise quantitativa não é justificável ou requerido (ABNT NBR 31010:2012).

Concluindo, apesar de conseguir todos os dados e valores necessários para realizarmos a análise de risco, o resultado sempre será uma estimativa e poderá apoiar a direção da empresa na tomada de decisão para gerenciar os riscos identificados, analisados e avaliados, decidindo sobre a melhor forma de tratamento destes riscos.

## MÉTODOS DE ANÁLISE DE RISCO – MÉTODO MOSLER (ATUALIZADO)

Neste artigo vamos falar sobre um dos métodos mais usados dentre aqueles que são subjetivos ou qualitativos que, ao contrário dos métodos objetivos ou quantitativos, não possuem históricos de ocorrências registrados. É o método Mosler.

Neste caso, vale-se muito mais da própria experiência, conhecimento técnico do gestor e análise de cenário, da conjuntura atual para, em conjunto com as demais pessoas que fazem parte da equipe que faz a análise de risco, pontuar (dar notas) os quesitos necessários deste método.

A avaliação do entorno do *"site"* estudado, e das ocorrências com empresas do mesmo porte ou segmento, principalmente aquelas localizadas na região, serão fundamentais para uma avaliação mais precisa, pois estaremos avaliando o cenário da região.

O princípio para metodologias de análise de riscos que não possuem históricos de ocorrências, como por exemplo, a abertura de uma nova filial, a fusão de empresas, etc., porém, nada impede que esta metodologia seja empregada em riscos já existentes e que possuem histórico, inclusive.

Principalmente naquelas situações onde houve a alteração do cenário estudado.

Para entender a importância dos métodos qualitativos, imagine a seguinte situação:

Você fez a análise de risco de uma agência bancária que já existe há muitos anos naquele local e sofreu uma série de roubos. Através do método estatístico, a análise indicou que a probabilidade de ocorrência de roubos neste ano (cinco roubos, por exemplo) é de 75%.

Ocorre que este mês, em frente a agência bancária analisada, foi criada uma companhia da Polícia Militar.

Fazendo a análise através dos números de ocorrência, com o método matemático, a probabilidade ainda seria de 75%. Os números não mudam.

Mas será que isso seria real nesta nova condição?

Com a análise realizada por métodos qualitativos, os analistas podem alterar suas avaliações de acordo com o novo cenário. No método estatístico não.

O método Mosler é muito empregado na segurança patrimonial e empresarial, principalmente nos países da Europa e no Brasil.

Mais uma vez, lembro da necessidade da colaboração de outras pessoas da empresa que possam auxiliar, principalmente na valoração dos bens tangíveis e intangíveis e na informação dos processos da empresa, facilitando, ao gestor, a visão dos riscos dos diversos processos.

É importante destacar que para gestão de riscos da empresa será necessário identificar qual a metodologia de avaliação de risco será utilizada, dentre as diversas possibilidades.

Estabelecer o contexto do processo de gestão de riscos inclui (.....) a definição das metodologias do processo de avaliação de riscos (ABNT NBR 31010:2012).

O método Mosler é uma metodologia cientifica, dividida em quatro fases, assim distribuídas:

Definição do risco (bem e o dano)

Análise do risco (seis critérios)

Evolução do risco

Classe do risco

A análise de risco é realizada através da mensuração de seis critérios.

Os critérios são:

**Critério da Função (F)** – projeta as consequências ou danos que podem alterar a atividade principal da empresa, caso o risco se concretize, na seguinte pontuação:

| Escala: | Pontuação: |
|---|---|
| Muito Gravemente | 05 |
| Gravemente | 04 |
| Medianamente | 03 |
| Levemente | 02 |
| Muito Levemente | 01 |

**Critério da Substituição (S)** – avalia qual o impacto da concretização da ameaça sobre os bens, ou seja, a dificuldade em substituir os bens atingidos. Sua escala de pontuação é:

| Escala: | Pontuação: |
|---|---|
| Muito Dificilmente | 05 |
| Dificilmente | 04 |
| Sem Muitas Dificuldades | 03 |
| Facilmente | 02 |
| Muito Facilmente | 01 |

**Critério da Profundidade (P)** – Caso o risco se concretize, mede a perturbação interna e os efeitos psicológicos que o risco poderá causar para a imagem da empresa. Possui a seguinte tabela de pontuação:

| Escala: | Pontuação: |
|---|---|
| Perturbações Muito Graves | 05 |
| Perturbações Graves | 04 |
| Perturbações Limitadas | 03 |

| | |
|---|---|
| Perturbações Leves | 02 |
| Perturbações Muito Leves | 01 |

**Critério da Extensão (E)** – mede o alcance e a **extensão** que o dano causaria à empresa, caso se concretizasse. Possui a seguinte escala de pontuação:

| Escala: | Pontuação: |
|---|---|
| De caráter Internacional | 05 |
| De caráter Nacional | 04 |
| De caráter Regional | 03 |
| De caráter Local | 02 |
| De caráter Individual | 01 |

**Critério de Agressão (A)** – Mede a possibilidade de o risco vir a ocorrer, de acordo com as características conjunturais e físicas da empresa onde a avaliação está sendo realizada. A tabela de avaliação é:

| Escala: | Pontuação: |
|---|---|
| Muito Alta | 05 |
| Alta | 04 |
| Normal | 03 |
| Baixa | 02 |
| Muito Baixa | 01 |

**Critério de Vulnerabilidade (V)** – Baseado no item anterior (critério de agressão), o critério da vulnerabilidade avalia o impacto financeiro caso o risco se concretize. Sua tabela de avaliação é a seguinte:

| Escala: | Pontuação: |
|---|---|

| | |
|---|---|
| Muito Alta | 05 |
| Alta | 04 |
| Normal | 03 |
| Baixa | 02 |
| Muito Baixa | 01 |

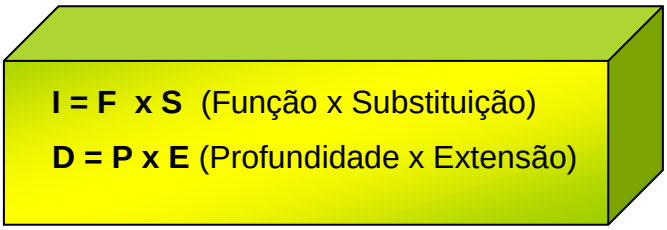
Para cada uma destes critérios, o gestor deve pontuar, de acordo com o cenário existente e sua experiência profissional. Sempre lembrando da necessidade da participação de outros integrantes da empresa para auxiliarem na avaliação desta pontuação.

Evolução do risco:

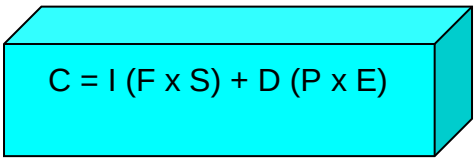
Agora veremos a Evolução do Risco, que é a quantificação do risco. Isto é feito calculando-se a magnitude do risco, representado pela letra "**C**".

O valor da magnitude do risco (**C**) é encontrado através da soma da **Importância do Sucesso** (**I**) e dos **Danos Causados** (**D**).

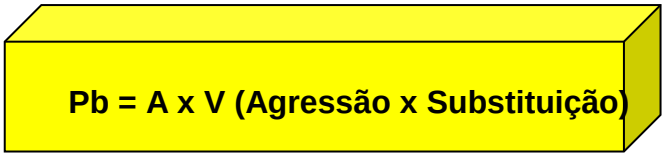
Então, a fórmula fica: C = I + D, onde:



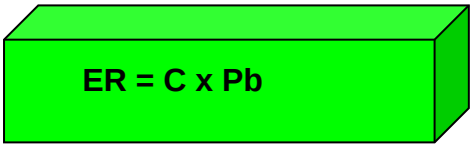

Desse modo a Magnitude do risco fica assim representada:




A próxima etapa será calcular a **Probabilidade de Ocorrência** (**Pb**), que será encontrada através da multiplicação da **Agressão** pela **Vulnerabilidade,** ficando assim representado:




Agora poderemos calcular a **Evolução do Risco** (**ER**) que é a multiplicação dos dois resultados encontrados anteriormente, o **C x Pb** (Magnitude do Risco x Probabilidade).




Com o resultado desta multiplicação encontramos o valor da Evolução do Risco, agora, a partir deste resultado, vamos classificar o risco.

Classe do risco

A classificação do risco nada mais é do que pegarmos o resultado do **ER** (Evolução do risco) e compará-lo com a tabela abaixo, classificando, dessa forma, o risco analisado.

De acordo com esta tabela a classificação pode ser:

| Valor do ER | Classe do Risco |
|---|---|
| 2 – 250 | Muito Baixo |
| 251 – 500 | Pequeno |
| 501 – 750 | Normal |
| 751 – 1.000 | Grande |
| 1.001 – 1.250 | Elevado |

A classificação do risco, de acordo com a análise realizada, dará subsídios para que o gestor possa priorizar as ações de segurança na empresa.

Este método pode ser representado através de uma grade que representa toda a metodologia, como vemos na tabela abaixo:

| Risco | F | S | P | E | A | V | I<br>F x<br>S | D<br>P x<br>E | C<br>I+D | Pb<br>A x V | ER<br>C x Pb | CLASSE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ASSALTO | 3 | 2 | 4 | 3 | 3 | 4 | 6 | 12 | 18 | 12 | 216 | MUITO BAIXO |

Apenas como exemplo, inseri alguns números na grade a fim de demonstrar sua utilização e o resultado alcançado.

É, sem dúvida, um método simples e que é usado há muito tempo na segurança patrimonial e empresarial, porém este método é subjetivo e seu resultado dependerá do grau de conhecimento do gestor e dos demais membros da empresa que colaboraram com a análise.

**Parametrização**

Apesar de esta metodologia ser usada amplamente na Europa, temos algumas dificuldades na sua aplicação, principalmente por apresentar como resultado conclusivo uma avaliação de que o risco pode ser muito baixo, pequeno, normal, grande ou elevado, ou seja, não é mensurável, o que dificulta a sua aceitação por parte dos empresários.

A partir destas dificuldades é que o professor Antonio Celso Ribeiro **Brasiliano,** criou a **parametrização**, que nada mais é do que transformar o resultado da classe do risco em percentual, ou seja, em probabilidade numérica, como ocorre com o método estatístico, o que facilita nosso entendimento e principalmente, a visualização do risco.

Além disso, ele substituiu o critério de agressão por probabilidade e de vulnerabilidade por impacto financeiro, permanecendo as mesmas tabelas de gradação.

Estas alterações no método Mosler ficaram conhecidas como método Brasiliano, devido à iniciativa do professor, porém hoje em dia ele usa uma metodologia própria dentro de um processo que segue o modelo sugerido pela ISO 31000.

Para fazer a parametrização é necessário pegar o resultado da análise da Evolução do Risco **(ER)** e classificá-lo na tabela de **Pb**, que é dividida em cinco níveis relativos à variação de faixa, que neste caso é de 20% (4% para cada faixa).

Por que 20%?

Porque são cinco faixas, que multiplicadas por 20% resultará nos 100% possíveis.

| Classe do Risco | Percentual |
|---|---|
| Elevado | 80,01% - 100% |
| Grande | 60,01% - 80% |
| Normal | 40,01% - 60% |
| Pequeno | 20,01% – 40% |
| Muito Baixo | 0 – 20% |

**Tabela de Probabilidade** – veja que é a mesma gradação da tabela de agressão, a qual ela substituiu.

| Escala: | Pontuação: |
|---|---|
| Muito Alta | 05 |
| Alta | 04 |
| Normal | 03 |
| Baixa | 02 |
| Muito Baixa | 01 |

Como no exemplo nós demos a menção 03 para agressão vamos mantê-la para probabilidade.

Então 3 x 4(%) = 12%

Também mantendo o resultado da **ER,** que ficou em 216 na classe MUITO BAIXA.

| Muito Baixo | 0 – 20% |
|---|---|

Assim, nós somaremos o valor inicial da porcentual da ER, neste caso 0 com a nota 3 que havíamos dado para a probabilidade (agressão), que multiplicado por 4 ficará 0 + 12 = 12% de probabilidade de concretização do risco.

Tabela resumo:

| Qualificação do risco | Nível de criticidade | Probabilidade | Tabela Pb |
|---|---|---|---|
| 2 – 250 | Muito baixo | 0 – 20% | 20% |
| 251 – 500 | Pequeno | 20,01% – 40% | 16% |
| 501 – 750 | Normal | 40,01% – 60% | 12% |
| 751 – 1000 | Grande | 60,01% – 80% | 8% |
| 1001 - 1250 | Elevado | 80,01% – 100% | 4% |

Quais são as vantagens em usar a parametrização?
Basicamente, ela simplifica a forma de analisarmos o resultado, apresentando percentuais de probabilidade.
Também podemos usar este resultado, que multiplicado pelo valor do impacto financeiro, nos dará a Perda Esperada, ou seja, o valor máximo do investimento para mitigar o risco analisado.

Esta é uma das metodologias possíveis para a realização da análise de risco, a qual sempre dependerá do tipo de negócio, da maturidade da equipe de avaliação, do tipo de risco envolvido, etc.
A análise de riscos consiste na determinação das consequências e suas probabilidades para eventos identificados de risco, levando em consideração a presença (ou não) e a eficácia de quaisquer controles existentes. As consequências e suas probabilidades são então combinadas para determinar um nível de risco (ABNT NBR 31010:2012).


## MÉTODO DE ANÁLISE DE RISCO – T. FINE

A gestão de riscos é uma ferramenta essencial para a elaboração dos planos de segurança de qualquer tipo de negócio.

A gestão de riscos é um processo que envolve a participação de diversas pessoas e não só do gestor de segurança e possui, dentro deste processo, a avaliação de riscos, que consiste na identificação dos riscos, na análise dos riscos identificados que determinará o impacto e a probabilidade de cada risco identificado e a avaliação dos riscos que, normalmente, apresentará uma matriz de risco a qual tem o objetivo de apoiar a tomada de decisão sobre o tratamento que será dado a cada risco.

A maneira como este processo é realizado é dependente não somente do contexto do processo de gestão de riscos, mas também dos métodos e técnicas utilizados para conduzir o processo de avaliação de riscos (ABNT NBR 31010:2012).

Neste artigo veremos o método de análise de riscos Willian T. Fine, que é um método semiquantitativo e permite identificar os riscos e hierarquizar os mesmos, de forma a apoiar a decisão em aplicar as medidas corretivas que poderão ser instauradas. O método foi publicado em 1971 e posteriormente foi adaptado.

Esta metodologia acrescenta como diferencial a Justificativa de investimento, que é uma forma de mostrar sua limitação econômica para aprovação do projeto.

Lembro da necessidade da colaboração de outras pessoas da empresa que possam auxiliar, principalmente na valoração dos bens e na informação dos processos das empresas, facilitando, ao gestor, a visão dos riscos nos diversos processos.

O Método T. Fine também é baseado, assim como o método Mosler, em critérios de avaliação, cada um deles com uma escala de valor. Métodos qualitativos são importantes, principalmente para empresas que não possuam histórico de ocorrências, porém é necessária uma boa avaliação dos impactos econômicos para realizar uma boa análise.

O objetivo deste método é encontrar o **Grau de Criticidade** a partir dos critérios de avaliação deste método.

De acordo com o Grau de Criticidade, o gestor saberá determinar a urgência com que o risco deve ser tratado.

No método T. Fine os critérios de avaliação, são:

**C = Consequência** – são os impactos tanto econômicos como pessoais decorrentes da concretização da ocorrência.

Neste critério devem ser acrescidos todos os impactos financeiros decorrentes da concretização de um determinado risco.

Esse impacto financeiro será inserido em uma tabela de consequências, a qual deve ser formulada pela empresa, apenas adequando a sua classificação, como veremos mais adiante.

**E = Exposição** - este critério avalia a frequência com que o evento ocorre na empresa ou em empresas similares, pois nem sempre teremos os dados da empresa avaliada.

Como dissemos, este método é muito utilizado nas empresas que não possuem histórico de ocorrências. Neste caso, devem-se avaliar empresas similares da região a fim de poder classificar a exposição ao risco, de acordo com a sua tabela.

**P = Probabilidade** – é a avaliação da real chance de o evento vir a ocorrer em um determinado espaço de tempo.
Mais uma vez será necessária a avaliação de empresas similares para encontrar a classificação adequada quanto à probabilidade do risco se concretizar, caso a empresa não tenha histórico de ocorrências deste tipo.

**GC = Grau de Criticidade** - a fórmula para encontrarmos o Grau de Criticidade é bem simples, bastando multiplicar o valor da Consequência pelo valor da Exposição e pelo valor da Probabilidade.

A fórmula do GC é:


Os valores para cada critério serão baseados nas tabelas que seguem:

C = Consequência:

| Classificação | Valor |
|---|---|
| Quebra da atividade fim da empresa, danos superiores a US$ 1 milhão. | 100 |
| Dano ente US$ 500 mil e US$ 1 milhão. | 50 |
| Dano entre US$ 100 mil e US$ 500 mil. | 25 |
| Dano entre US$ 1 mil e US$ 100 mil. | 15 |
| Danos abaixo de US$ 1 mil. | 5 |
| Pequenos danos. | 1 |

**Observação:** esta tabela deve ser adaptada de acordo com a empresa porque o que, por exemplo, US$ 10 milhões representam para o negócio de uma empresa pode ser bem diferente para outra empresa menor ou maior. Esta é a razão da necessidade de adaptação da tabela de acordo com a empresa.

Caso isso não seja levado em consideração toda a análise será perdida ou se tornará inviável, sem nenhuma praticidade.

E = Exposição:

| Classificação | Valor |
|---|---|
| Várias vezes ao dia. | 10 |
| Uma vez ao dia - frequentemente. | 5 |
| Uma vez por semana ou ao mês - ocasionalmente. | 3 |
| Uma vez ao ano ou ao mês - irregularmente. | 2 |
| Raramente possível - sabe-se que ocorre, mas não com frequência. | 1 |
| Remotamente possível - não sabe se já ocorreu. | 0,5 |

P = Probabilidade:

| Classificação | Valor |
|---|---|
| Espera-se que aconteça. | 10 |
| Completamente possível – 50% de chance de ocorrência. | 6 |
| Coincidência se ocorrer. | 3 |
| Coincidência remota – sabe-se que já ocorreu. | 1 |
| Extremamente remota – porém possível | 0,5 |
| Praticamente impossível – uma chance em um milhão. | 0,1 |

**Tratamento do risco -** de acordo com as tabelas apresentadas, o Grau de Criticidade será o resultado da multiplicação direta dos três critérios.
Com este resultado (GC) vamos procurar na tabela a seguir, qual o tratamento deverá ser adotado pelo gestor.

O tratamento do risco segue a seguinte tabela:

| Grau de Criticidade | Tratamento do Risco |
|---|---|
| Maior ou igual a 200 | Correção imediata – risco tem que ser reduzido. |
| Menor que 200 e maior que 85 | Correção urgente – requer atenção. |
| Menor que 85 | Risco deve ser monitorado. |

Baseado no resultado, o gestor poderá adotar as medidas necessárias para atuar na mitigação dos riscos analisados.

A grande parte dos riscos alcança entre 85 e 200 na tabela de tratamento, as quais necessitam de correção urgente ou requer correção urgente e requer atenção e tratamento.

Os riscos menores de 85 devem ser apenas monitorados, pois podem ter um grande impacto financeiro, porém com poucas chances de concretização, sendo seu monitoramento necessário a fim de acompanhar sua possível evolução.

Lembremos que os riscos são essencialmente dinâmicos, necessitando de monitoramento constante.

Justificativa de Investimento:

A partir da elaboração da análise para que o gestor possa priorizar o tratamento dos riscos, vamos buscar a Justificativa de Investimento, a qual deve estar diretamente relacionada com o Grau de Criticidade.

Este método dará ao gestor, os parâmetros necessários para o investimento em segurança.

Fator de Custo:

O Fator de Custo é o valor que será investido na segurança para tratar o risco analisado.

Este valor inclui equipamentos, treinamentos, contratações, enfim, tudo o que for necessário para tratar o risco.

Ele é apresentado na seguinte tabela:

| 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 |

É claro que esta tabela também pode ser adaptada de acordo com a empresa e, principalmente, se o gestor alterou a tabela de Consequências, tornando-a mais pratica, de acordo com o negócio analisado.

Grau de Correção

Este é o critério mais importante para o gestor, pois aqui ele irá calcular o quanto é possível mitigar o risco usando o investimento que ele dispõe.

Aqui é que a experiência da equipe que faz a análise de riscos e os estudos realizados para avaliar os critérios que compõem o Grau de Criticidade, além da conjuntura global da empresa, será posta à prova. Caso o estudo não tenha sido criterioso e bem avaliado, o resultado não será satisfatório.

Além disso, o gestor não terá argumentos para criar as metas para mitigação dos riscos.

| 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 |

Justificativa de Investimento:

A fórmula para saber se o investimento proposto é justificado é:

$$JI = \frac{GC}{\text{Fator de Custo x Grau de Correção}}$$

O resultado desta fórmula é o Índice de Justificação.
Ele é apresentado em valor numérico, o qual será inserido numa outra tabela, chamada de Escala de Valoração do **Índice de Justificação.**

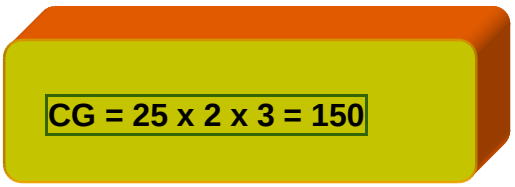
Exemplo:
Para facilitar o entendimento, vamos exemplificar um caso, simplificado, de um estudo.

Numa empresa que precisa diminuir suas perdas num valor de US$ 150.000 de um determinado risco, onde haverá um investimento de US$ 45.000.
A mitigação proposta do risco seja de 75%.
O risco estudado já ocorreu uma vez.
Usando o método T. Fine, a fórmula ficaria assim:

Grau de Criticidade:

**GC = C x E x P**

C = 25
E = 2
P = 3




De acordo com a tabela de Tratamento de Risco, o tratamento requer atenção, correção urgente.

Justificativa de Investimento:

$$JI = \frac{GC}{\text{FC x G. Correção}}$$

GC = 150

FC = 6

GC = 3

$$JI = \frac{150}{(US\$\ 45.000)\ 6 \times (75\%)\ 2}$$

**JI = 12,5**

Para sabermos se o resultado da Justificativa de Investimento é compatível com o Grau de Criticidade, ou seja, se o investimento é justificado ou não, devemos usar uma outra tabela, que é a da Escala de Valoração.

Escala de Valoração:

Nesta tabela estão inseridos os valores do Índice de Justificação e o resultado deste investimento.

A associação Americana de Gerenciamento de Riscos estabeleceu como padrão em 1976, a tabela abaixo, para avaliarmos se o investimento será justificado ou não.

| Escala de Valoração do Índice de Justificação | |
|---|---|
| FATOR 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. |

De acordo com esta tabela, o resultado do exemplo apresentado (12,5) é normalmente justificado.

Assim, o método T. Fine, apesar de ser amplamente usado, representa sua probabilidade de uma maneira que pode dificultar o convencimento dos empresários para justificar a implementação de um projeto de segurança.
Da mesma forma que foi feito para o método Mosler, o professor Antonio Celso Ribeiro **Brasiliano,** parametrizou este resultado, transformando-o em porcentagem, pois tem um maior grau de facilidade no entendimento.
Este processo de parametrização, transforma o resultado subjetivo num resultado objetivo.
A parametrização para o método T. Fine funciona da seguinte forma:
Deve-se pegar a tabela de Tratamento do Risco e dividir o total possível, ou seja, 100% pela quantidade de divisões existentes, no caso, três, conforme exemplificado na tabela abaixo.
(100 ÷ 3 = 33,33)

| Grau de Criticidade | Tratamento do Risco | Total - 100% |
|---|---|---|
| GC maior ou igual a 200 | Correção imediata – risco tem que ser reduzido. | 66,68% - 100% |
| GC menor que 200 e maior que 85 | Correção urgente – requer atenção. | 33,34% - 66,67% |
| GC menor que 85 | Risco deve ser monitorado. | 0% - 33,33% |

Para a tabela de Probabilidade, nós dividiremos o valor de uma faixa de percentual, ou seja, 33,33% e agora vamos dividir este valor pelo número de faixas existentes na tabela de probabilidade, no caso, seis.
A tabela fixará assim descrita:

(33,33 ÷ 6 = 5,56)

| Classificação | Valor | Total - 33,33% | Nota da Pb |
|---|---|---|---|
| Espera-se que aconteça. | 10 | 33,33% | 6 |
| Completamente possível – 50% de chance de ocorrência. | 6 | 27,80% | 5 |
| Coincidência se ocorrer. | 3 | 22,24% | 4 |

| | | | |
|---|---|---|---|
| Coincidência remota – sabe-se que já ocorreu. | 1 | 16,68% | 3 |
| Extremamente remota – porém possível | 0,5 | 11,12% | 2 |
| Praticamente impossível – uma chance em um milhão. | 0,1 | 5,56% | 1 |

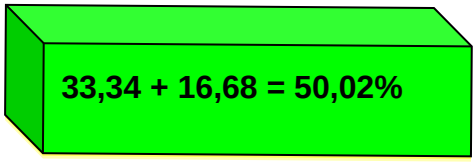
Para facilitar o entendimento, inseri a coluna com a nota da avaliação dada à probabilidade.

Seguindo e exemplo do estudo apresentado, a nota para a Probabilidade foi 6 e o resultado do Grau de Criticidade do estudo foi 150 (correção urgente).

Neste caso, vamos pegar sempre o menor valor da faixa criada com a divisão do 100%, na tabela de tratamento do risco, que no caso exemplificado foi de 150 (correção urgente) onde o menor valor é 33,34%.

Na tabela de probabilidade a nota 6 corresponde a 33,33%

Este valor (33,34%) somado a nota que demos para a Probabilidade, que foi 3, que representa na tabela de Probabilidade 16,68% (5,56 x 3) resultará em:




Dessa forma, a Probabilidade que era representada apenas pela expressão “Coincidência se ocorrer” passa a ser representada por 50,02%.

Com este resultado podemos calcular a perda esperada, que é a multiplicação do impacto financeiro com a probabilidade.

Ainda usando o resultado do exemplo citado, o valor da perda esperada será:

US$ 150.000 x 50.02% = US$ 75.030.

O valor da perda esperada é o investimento máximo que pode ser feito para o risco exemplificado.

O processo de avaliação de riscos pode ser conduzido em vários graus de profundidade e detalhe e utilizando um ou muitos métodos que vão do simples

ao complexo. Convém que a forma de avaliação e sua saída sejam compatíveis com os critérios de risco, desenvolvidos como parte do estabelecimento do contexto (ABNT NBR 31010:2012).

Cada negócio tem as suas características e nem sempre a metodologia de análise de risco será aplicável para todas as situações.

Cabe ao gestor a escolha, de acordo com o negócio, da metodologia que trará maior resultado e eficácia ao projeto de segurança.


## MÉTODO BRASILIANO (BÁSICO) PARA ANÁLISE DE RISCOS

Hoje a gestão de riscos é reconhecida como parte integrante de uma boa administração. Trata-se de um processo interativo composto por etapas que, quando realizadas em sequência, possibilitam a melhoria da tomada de decisão.

Neste artigo vamos tratar do Método Brasiliano, criado pelo professor Antonio Celso Ribeiro Brasiliano e que assim como outras metodologias, é qualitativo/subjetivo e depende da avaliação e percepção das pessoas envolvidas. Os métodos qualitativos são essenciais para os casos de riscos que não possuem histórico de ocorrência.

Há, porém, uma diferença essencial, que é o fato de ter sido criado por um brasileiro com ampla experiência na utilização dos métodos mais tradicionais, o que lhe garante grande confiabilidade e que possui uma sequência mais prática e completa.

O método é dividido em quatro partes, sendo:

1) Identificação dos fatores de riscos;

2) Determinação do grau de probabilidade;

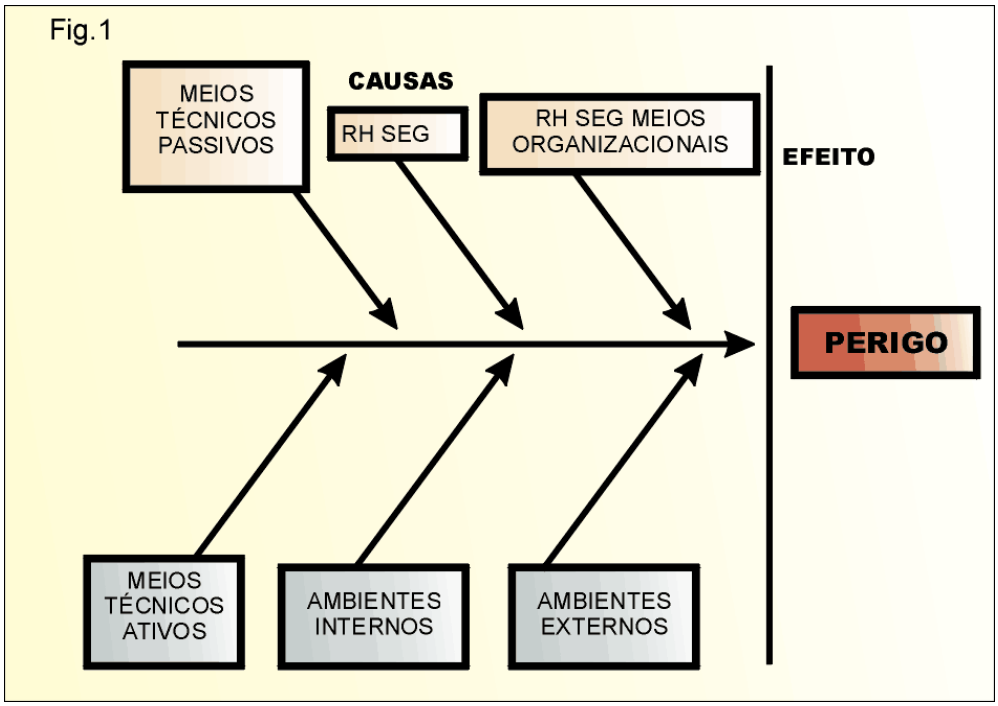
3) Determinação do impacto financeiro;

4) Elaboração da perda esperada e matriz de vulnerabilidade.

1) Identificação dos fatores de riscos

Os fatores de riscos são as causas, ou seja, a origem dos riscos. Assim, adaptou-se o diagrama de Ishikawa também conhecido por espinha de peixe (abordado no Jornal da Segurança, na edição 144). Os fatores de risco que originalmente eram os seis “M” (Medidas, Meio Ambiente, Mão-de-obra, Materiais, Métodos e Máquinas), foram substituídos por seis fatores diferentes: Meios Organizacionais; Recursos Humanos da Segurança; Meios Técnicos

Passivos; Meios Técnicos Ativos; Ambiente Interno; Ambiente Externo. Dessa forma, o diagrama de causa e efeito ficou assim:




Onde: “Meios Organizacionais”: corresponde ao levantamento de normas de rotina e de emergência, políticas de tratamento de riscos, gerenciamento de riscos, entre outras. A formalização ou o não detalhamento pode ser um fator de influência para a concretização do risco;

“**Recursos Humanos da Segurança**”: é o levantamento do nível de qualificação, quantidade, posicionamento tático da equipe de segurança;

“**Meios Técnicos Passivos**”: é o levantamento da falta de recursos físicos, tais como layout de portaria, salas, resistências de paredes, vidros, etc;

“**Meios Técnicos Ativos**”: levantamento da falta de sistemas eletrônicos, como CFTV, controle de acesso, sensoriamento, sistemas de rastreamento e centrais de segurança;

“**Ambiente Interno**”: levantamento do nível de relacionamento dos colaboradores e empresa. Inclui desde políticas de remuneração até políticas de recursos humanos. É a ambiência da empresa; e, finalmente,

“**Ambiente Externo**”, que é o levantamento de cenários prospectivos, identificando fatores externos incontroláveis, mas que influenciam a concretização dos riscos. Inclui o levantamento dos índices de criminalidade,

estrutura do crime organizado, mercados paralelos, estrutura do judiciário, corrupção policial, ambiência no entorno, entre outros.

O diagrama estabelece a relação entre as causas e o efeito e possibilita um detalhamento das causas, facilitando a elaboração do plano de ação. Esta primeira etapa do método é fundamental para a realização da análise de risco. Caso ela seja negligenciada, o resultado da análise estará comprometido.

2) Determinação do grau de probabilidade

O grau de probabilidade (GP) é a consequência da multiplicação dos fatores de riscos versus e o critério da exposição. É uma multiplicação direta, onde cada critério possui uma escala de valoração de 1 a 5.

O fator de risco (FR), possui seis critérios: Meios Organizacionais, Recursos Humanos da Segurança, Meios Técnicos Passivos, Meios Técnicos Ativos, Ambiente Interno e Ambiente Externo e serão avaliados de acordo com sua influência para que o risco analisado se concretize.

Esta avaliação deve ser feita de acordo com uma tabela que servirá de parâmetro para todos os fatores de risco. Cada fator de risco possui uma escala de valoração que indica o quanto este critério influencia a concretização do risco.

A escala de valoração usada para cada um dos critérios possui a seguinte gradação, como mostra a tabela 1:

| ESCALA | PONTUAÇÃO |
|---|---|
| Influencia muito | 05 |
| Influencia | 04 |
| Influencia medianamente | 03 |
| Influencia levemente | 02 |
| Influencia muito levemente | 01 |

Para encontrar o grau final do critério “fator de risco”, basta somar os seis critérios e dividir por seis, ou seja, tirar a média aritmética.

Supondo que tivéssemos avaliado um risco e as pontuações alcançadas fossem como mostra a tabela 2, a soma da pontuação seria 21.

Este resultado será dividido pelo número de fatores (6) e revela que o critério “fator de risco” possui um nível de influência de 3,50. (Tabela 2)

| Fatores de risco | Pontuação |
|---|---|
| Meios Organizacionais (MO) | 04 |
| Recursos Humanos da Segurança (RH) | 03 |
| Meios Técnicos Passivos (MTP) | 04 |
| Meios Técnicos Ativos (MTA) | 03 |
| Ambiente Interno (AI) | 05 |
| Ambiente Externo (AE) | 02 |

Critério da exposição (E) é a frequência que o risco costuma manifestar-se na empresa ou em empresas similares. Possui a seguinte escala de gradação: (Tabela 3)

| ESCALA | PONTUAÇÃO |
|---|---|
| várias vezes ao dia | 05 |
| freqüentemente | 04 |
| ocasionalmente | 03 |
| irregularmente | 02 |
| remotamente | 01 |

Para completar o exemplo, vamos conferir a pontuação 05 hipoteticamente.

Para encontrar o grau de probabilidade (GP) é necessário multiplicar os resultados dos fatores. A fórmula é: GP (grau de probabilidade) = FR (fator de risco) x E (exposição).

Partindo do exemplo acima, o resultado será: GP = 3,50 X 5 = 17,50

Para saber sua classificação, deve-se consultar a tabela de classificação da probabilidade (tabela 4):

| ESCALA | Nível de risco | Probabilidade de concretização |
|---|---|---|
| 1-5 | BAIXA | 4% a 20% |
| 5,01 - 10 | MÉDIA | 20,01% a 40% |
| 10,01 - 15 | ALTA | 40,01% a 60% |
| 15,01 - 20 | MUITO ALTA | 60,01% a 80% |
| 20,01 - 25 | ELEVADA | 80,01% a 100% |

Neste exemplo, o Grau de Probabilidade (GP) é de 17,50, que na tabela representa um nível “muito alto”, ou ainda entre 60,01% e 80% de probabilidade do risco se concretizar.

Para transformar esta classificação subjetiva em uma classificação mais 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 risco x fator de exposição) que é 25 na escala, e a probabilidade máxima que é 100%.

Seguindo o exemplo citado, o resultado será 17,50 x 4 = 70%

Isso quer dizer que a probabilidade do risco se concretizar ou de continuar a acontecer na empresa é de 70%.

3) Determinação do impacto financeiro

Nesta etapa, devemos projetar todos os custos que os riscos causam de impacto nos negócios da empresa, levantando as consequências diretas e

indiretas.

O investimento que servirá de parâmetro para tratar o risco será fruto da multiplicação direta entre a probabilidade de ocorrência de cada risco com o seu impacto financeiro, pois nesse caso encontraremos o custo da Perda Esperada, que é um parâmetro usado para representar o investimento máximo que deve ser realizado pela empresa para mitigar determinado risco.

Quando o investimento for maior do que o da perda esperada, significa que o investimento foi supra dimensionado, ou seja, está se gastando mais para proteger do que o valor do bem protegido.

O Método Brasiliano sugere a realização de um estudo baseado no levantamento dos custos prováveis, caso determinado risco venha a acontecer.

Daí a importância da participação de uma equipe multidisciplinar na avaliação do risco. Setores como produção, marketing, financeiro e outros, de acordo com o risco analisado e a estrutura da empresa, são fundamentais na composição desta equipe para que a análise atenda às expectativas da empresa e o gestor ganhe credibilidade para a implantação do projeto de segurança.

As informações que devem ser levantadas em todos os departamentos são as seguintes:

**Substituição permanente (Sp)** - onde se enquadram os custos definitivos, ou seja, equipamentos, instalações, salários, indenizações, que a empresa não obterá mais;

b) **Substituição temporária (St)** - onde se enquadra o que a empresa perde temporariamente, como aluguel de equipamento, instalação, tempo de funcionários parados, etc.

c) **Custo consequente (Cc)** - avalia que prejuízo o risco deu à corporação, como queda de faturamento, imagem da empresa, etc.

d) **Redução de dinheiro em caixa (Rc)** - diz respeito à redução efetiva do numerário em caixa, em casos de assalto, incêndio, entre outros.

e) **Indenização do seguro (I)** - neste item é levantado quanto o seguro irá pagar para a empresa, caso ocorra o sinistro.

f) **Prêmio pago até o momento do sinistro (P)** - neste item é levantado quanto a empresa já pagou, em parcelas mensais, à seguradora.

De forma metodológica, é possível avaliar o custo das perdas reais e potenciais, pela fórmula**:**

**CP = Sp + St + Cc + Rc – ( I – P )**

O resultado (CP) será o Custo da Perda, representado em valores monetários (R$ ou US$), de acordo com a empresa.

Para exemplificar:

Uma empresa, após os levantamentos necessários chegou aos seguintes valores, caso houvesse um incêndio no depósito XY-1:

Sp = R$ 230 mil

St = R$ 320 mil

Cc =R$ 450 mil

Rc = R$ 60 mil

I = R$ 350 mil

P = R$ 1.500/mês (já pagou 6 meses) = R$ 9 mil

CP = 230 mil + 320 mil + 450 mil + 60 mil – (350 mil – 9 mil = 341 mil)

CP = R$ 719 mil, ou seja, este é o custo da perda, caso o sinistro ocorra.

O ideal é que a empresa tenha uma tabela de classificação do impacto financeiro nos negócios. A tabela 5, exemplificada abaixo, divide o impacto financeiro em valores significativos para a empresa.

| CLASSIFICAÇÃO | CUSTO (US$ ou R$) |
|---|---|
| CATASTRÓFICO | ACIMA DE 1.000.000,00 |
| SEVERO | 600.001,00 - 1.000.000,00 |
| MODERADO | 300.001,00 - 600.000,00 |
| LEVE | 200.000,00 - 3000.000,00 |

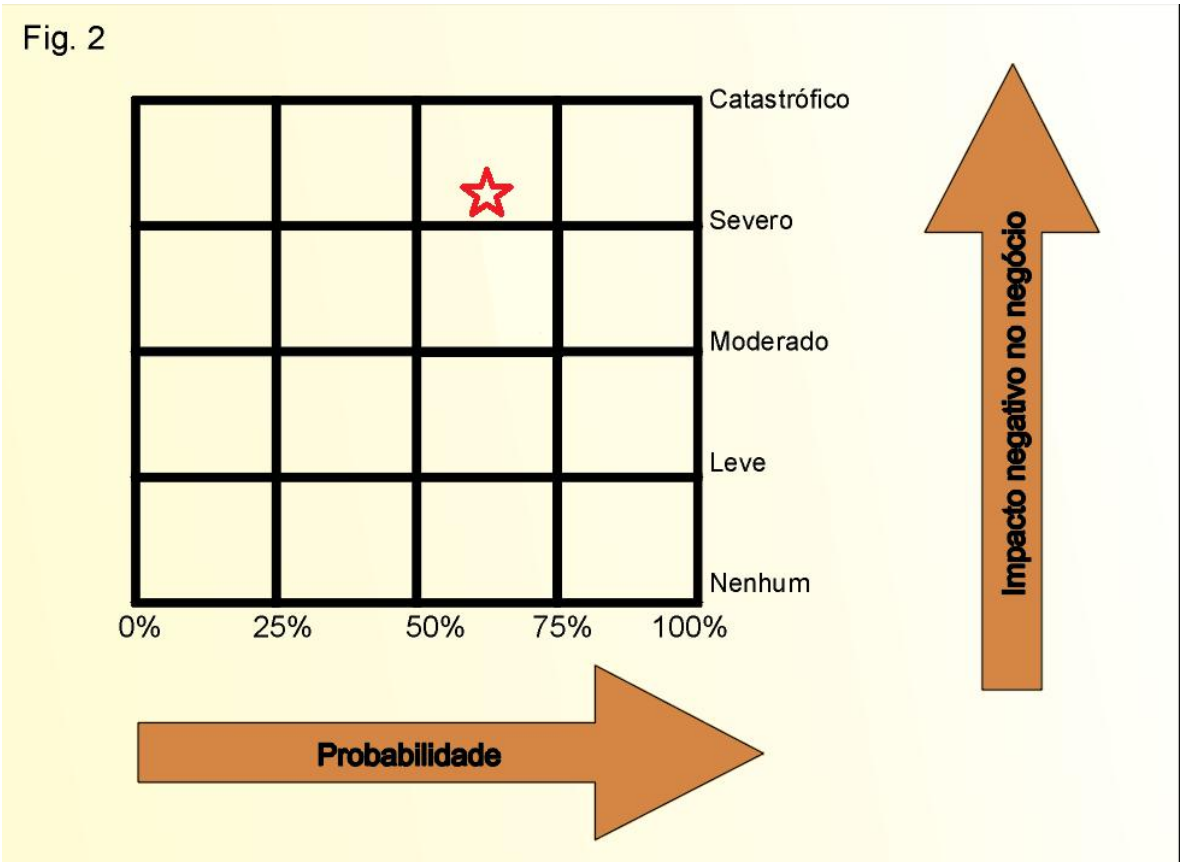
Obs: Logicamente, cada empresa tem sua própria tabela, motivo pelo qual a tabela apresentada é apenas ilustrativa.

A Perda Esperada (PE) é o cálculo para que se possa realizar uma relação custo-benefício equilibrada. A multiplicação do impacto financeiro pela probabilidade de ocorrência, acaba por equilibrar a chance de ocorrência com seu impacto.

A obtenção da perda esperada pode ser demonstrada através da matriz de vulnerabilidade. Dessa forma, ficam mais claros o posicionamento dos riscos analisados e seus impactos financeiros.

Para o gestor, a matriz irá auxiliar a dar prioridade para o tratamento dos eventos. Nela, o cruzamento horizontal e vertical mostra o posicionamento do evento, como exemplo acima (Fig. 2).

Fig. 2

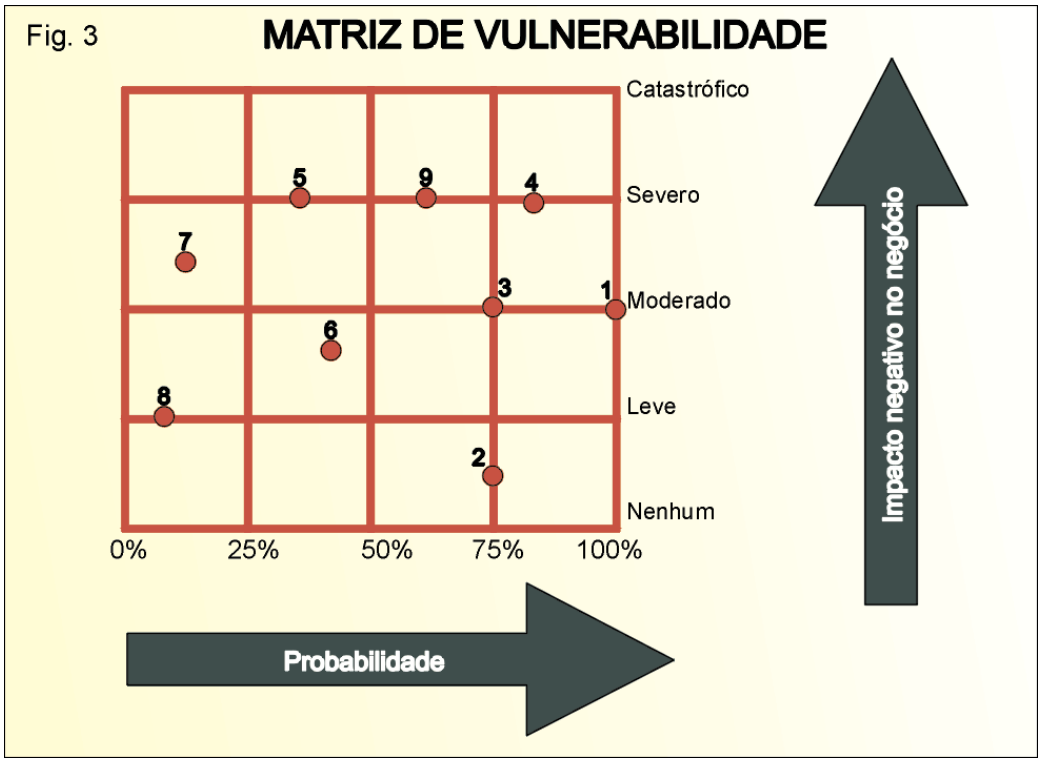



Nesse exemplo, o evento tem 70% de probabilidade de ocorrer e um custo de perda de R$ 719 mil. Para encontrar o valor da perda esperada, deve-se multiplicar R$ 719 mil por 70%. Nesse caso o valor da perda esperada é de R$ 503.300,00.

Cada risco estudado levará em conta sua probabilidade e o impacto financeiro, porém todos eles serão inseridos na mesma matriz. A matriz de vulnerabilidade apresentará diversos pontos, tantos quantos forem os riscos analisados.

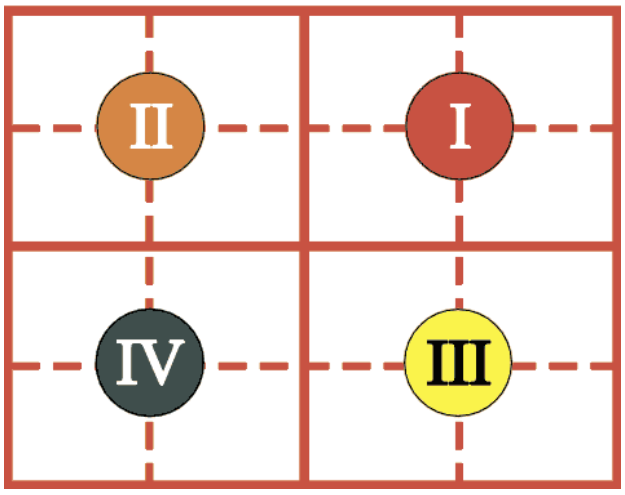
Na matriz ao lado (Fig 3), para exemplificar, há nove eventos inseridos, cada qual com a sua probabilidade e com o seu impacto financeiro para o negócio.

Fig. 3




Com a elaboração da matriz, é possível dividi-la em quatro partes, formando quatro quadrantes que serão utilizados para dar maior visibilidade às prioridades nas quais o gestor deverá atuar, levando em consideração a probabilidade da ocorrência e seu impacto para o negócio. Dessa forma, a matriz ficará assim dividida (Fig 4):

Fig. 4




Os quadrantes, chamados de quadrantes estratégicos, terão o seguinte tratamento:

Os riscos existentes no **quadrante I** são aqueles com alta probabilidade de ocorrência e podem resultar em impacto severo, caso ocorram. Portanto exigem a implantação imediata das estratégias de proteção e prevenção.

No **quadrante II** estão as ameaças que podem ser muito danosas à empresa, porém com menos probabilidade de ocorrer. Devem ser monitoradas de forma rotineira e sistemática.

No **quadrante III**, estão os riscos com alta probabilidade de ocorrência, mas que causam pouco dano à empresa. Estas ameaças devem possuir respostas rápidas, que devem estar planejadas e testadas em um plano de emergência.

No **quadrante IV**, a baixa probabilidade e o pequeno impacto representam pequenos problemas e prejuízos, devendo ser somente gerenciados e administrados no caso de ocorrência.

De acordo com o exemplo da matriz com vários eventos, os quadrantes estratégicos ficariam como mostra a tabela 6:

| QUADRANTE | EVENTO | TRATAMENTO |
|---|---|---|
| I | 1,3,4,9 | Tratamento imediato |
| II | 5,7 | Ação depende da evolução |
| III | 2 | Tratar com ação de emergência |
| IV | 6,8 | Impacto assimilável |

Com base nesta matriz é que as estratégias de proteção poderão ser validadas, pois o investimento nos programas de proteção e prevenção estará plenamente justificado, dependendo de sua influência nos resultados da empresa.

A matriz servirá para apoiar a decisão da empresa, demonstrando quais os riscos afetam o negócio e qual a probabilidade de eles se repetirem ou se concretizarem.

Assim, será mais fácil decidir sobre onde investir para tratar dos riscos plotados.


## PLANEJAMENTO TÁTICO DE SEGURANÇA

O planejamento tático da segurança empresarial tem por objetivo a realização de um estudo pratico de análise de riscos corporativos que afetem os ativos tangíveis e intangíveis da empresa.

Ele pode ser realizado pelo gestor de segurança da empresa, tendo em vista que ele é desenvolvido nos níveis intermediários da organização.

Nele deve ser comparado o custo X benefícios, sempre integrando os meios organizacionais, com a reformulação ou criação de normas e procedimentos, com os meios técnicos, sejam ativos ou passivos e os recursos humanos.

A integração destes três fatores (meios organizacionais, meios técnicos e recursos humanos) é primordial para que os objetivos pretendidos sejam atingidos, através da eficiência, eficácia e efetividade, que são esperadas de um planejamento de segurança.

Além disso, o planejamento tático deve estar alinhado às políticas de segurança da empresa, visando os objetivos empresariais.

O planejamento possui sete fases, as quais são:

- Identificação dos riscos reais e potenciais;
- Identificação dos fatores de risco;
- Elaboração do diagnóstico;
- Análise de risco;

- Classificação dos riscos;
- Plano de ação;
- Controle e avaliação.

**A primeira fase** deve ser composta por uma equipe multidisciplinar que deve identificar quais são os riscos aos quais a empresa está sujeita. Um destes métodos para identificação dos riscos é conhecido como brainstorm (em português, tempestade de ideias).

Mas por que unir um grupo de pessoas para identificar os riscos da empresa? Porque em grupo podemos ver todos os ângulos da empresa. É injusto imaginar que o gestor de segurança, ou quem estiver fazendo a análise de risco, tenha a obrigação de conhecer todos os processos - que podem ser inúmeros - e possa identificar os riscos que uma empresa está exposta. Daí a necessidade da participação de pessoas das diversas áreas, normalmente, recursos humanos, marketing, financeiro, produção e segurança.

**Na segunda fase**, precisamos encontrar quais são os fatores de risco.

O método mais comum adotado pelos gestores é o do Diagrama de Causa e Efeito, também chamado de Diagrama Espinha de Peixe, ou ainda de Diagrama de Ishikawa, em homenagem ao engenheiro japonês Kaoru Ishikawa, que utilizou esse diagrama pela primeira vez em 1943.

Este processo, além de ser muito eficaz, é simples e fácil de usar. Consiste em, a partir da identificação de um efeito indesejável, no nosso caso, o risco, fazer a pergunta “Por que?” Repetidamente, até estratificar todos os possíveis fatores.

Assim como foi criado para ser usado como uma das ferramentas da qualidade, também foi adaptado para uso na segurança. No método Brasiliano de Análise de Risco, por exemplo, foram sugeridas as seguintes categorias: Recursos Humanos da Segurança, Meios Organizacionais, Meios Técnicos Ativos, Meios Técnicos Passivos, Ambiente Interno e Ambiente Externo.

Onde:

**Meios Organizacionais –** é o levantamento se na empresa possui normas de rotina e de emergência, políticas de tratamento de riscos, gerenciamento de

riscos entre outras. A não formalização ou o não detalhamento pode ser um fator de influência para a concretização do perigo.

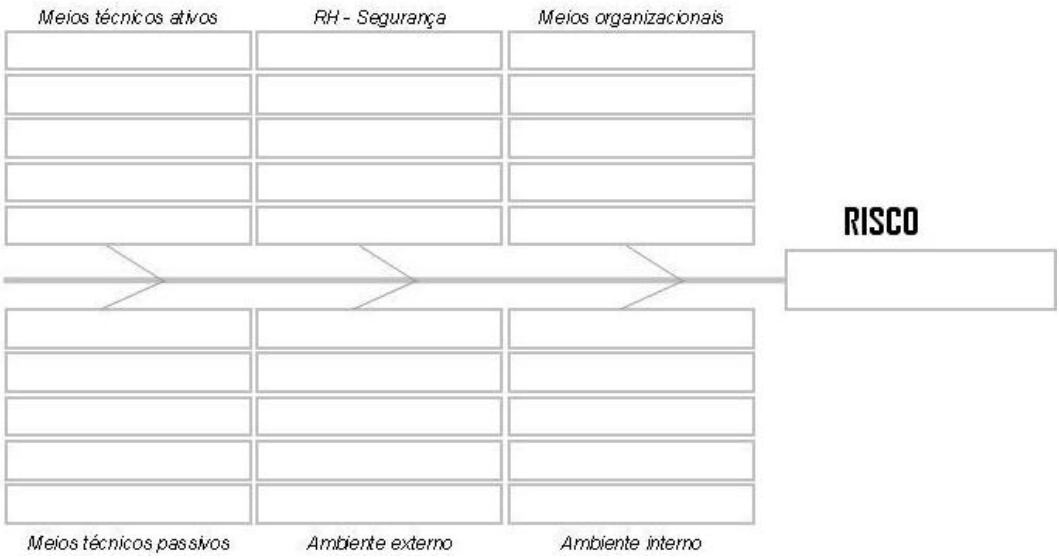
**Recursos Humanos da Segurança -** é o levantamento do nível de qualificação, quantidade, posicionamento tático da equipe de segurança.

**Meios Técnicos Passivos** - é o levantamento da falta de recursos físicos, tais como layout de portaria, salas, resistências de paredes, vidros entre outros.

**Meios Técnicos Ativos** - é o levantamento da falta de sistemas eletrônicos, como por exemplo: CFTV, controle de acesso, sensoriamento, sistemas de rastreamento e centrais de segurança.

**Ambiente Interno -** é o levantamento do nível de relacionamento dos colaboradores e empresa. Inclui desde políticas de remuneração até políticas de recursos humanos. É a ambiência da empresa.

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




O diagrama estabelece a relação entre as causas e o efeito e possibilita um detalhamento das causas, facilitando a elaboração do plano de ação.

Este diagrama é de fundamental importância para o planejamento tático, pois ele determinará quais as ações serão necessárias para diminuir a probabilidade de um determinado perigo se repetir.

Com ele é possível identificarmos as causas de uma determinada ocorrência, e é justamente nas causas que devemos atuar e não no efeito. Para maiores detalhes da primeira e segunda fase, veja a edição do Jornal da Segurança nº 144, onde publicamos um artigo sobre este assunto, especificamente.

**A terceira fase** é a elaboração do diagnóstico da empresa. É como se fosse uma fotografia da empresa, levantando seus pontos fortes e fracos, as oportunidades e ameaças.

Uma forma para fazermos este diagnóstico é usando a matriz SWOT, o termo SWOT vem do inglês e representa as iniciais das palavras Strenghts (forças), Weaknesses (fraquezas), Opportunities (oportunidades) e Threats (ameaças). Podemos usar o termo FOFA, que significa Forças, Oportunidades, Fraquezas e Ameaças.

A SWOT ou FOFA representada numa matriz fica desta forma:

MATRIZ SWOT - FOFA

| FORÇAS | OPORTUNIDADES |
|---|---|
| | |
| FRAQUEZAS | AMEAÇAS |

No quadrante das forças serão relacionados os pontos fortes da empresa, em relação a sua segurança e no quadrante das fraquezas serão inseridas as informações de suas vulnerabilidades, justamente aquelas apontadas na elaboração do diagrama de causa e efeito.

No quadrante de oportunidades serão relacionados pontos positivos para a empresa, mas que são de origem externa, ou seja, não dependem da empresa. Assim como no quadrante das ameaças, que também são externas e a empresa pode, no máximo, influenciar para evitá-las, mas são fatores externos a empresa.

Tudo que está relacionado nos quadrantes das forças e fraquezas dependem apenas da empresa.

Dessa forma teremos uma "fotografia" da empresa, focada nas suas condições de segurança e saberemos onde devemos agir para mitigar seus riscos, onde a empresa deve investir.

**A quarta fase** do planejamento tático consiste na análise de risco. A análise de risco busca duas informações básicas que são: qual a probabilidade do risco se concretizar ou de continuar acontecendo e qual o impacto que este evento traz para a empresa. Com esses resultados, probabilidade e impacto, podemos calcular a perda esperada, que é o investimento máximo que deve ser feito para o risco estudado.

Existem diversos métodos de análise de risco, basicamente, eles podem ser métodos objetivos ou subjetivos, também conhecidos como quantitativos e qualitativos. De qualquer forma, independentemente do método utilizado os objetivos serão os mesmos.

Os métodos mais utilizados no Brasil são:

Método estatístico;

Mosler;

T. Fine; e

Brasiliano.

Essas metodologias nós já publicamos, cada uma delas, passo a passo, aqui, no Jornal da Segurança nas edições nº 145 até a edição nº 148.

**A quinta fase** do planejamento tático é a classificação dos riscos, que trata do matriciamento dos riscos.

O resultado da análise de risco nos dá condições de inserirmos esses resultados numa matriz, chamada de matriz de vulnerabilidade, caso tenhamos

os dados de forma objetiva ou então podemos utilizar a matriz de suportabilidade ou aceitabilidade, usadas principalmente nos casos onde a empresa não consegue mensurar suas perdas.

Matrizes:

As matrizes são ferramentas do gerenciamento de riscos que podem e devem ser utilizadas pelos gestores de segurança a fim de facilitar a tomada de decisão.

Elas são representadas de diversas formas e com diversas finalidades sendo que, basicamente, apresentam uma espécie de fotografia da situação da empresa em relação aos riscos analisados, indicando quais são os mais críticos e que merecem atenção imediata.

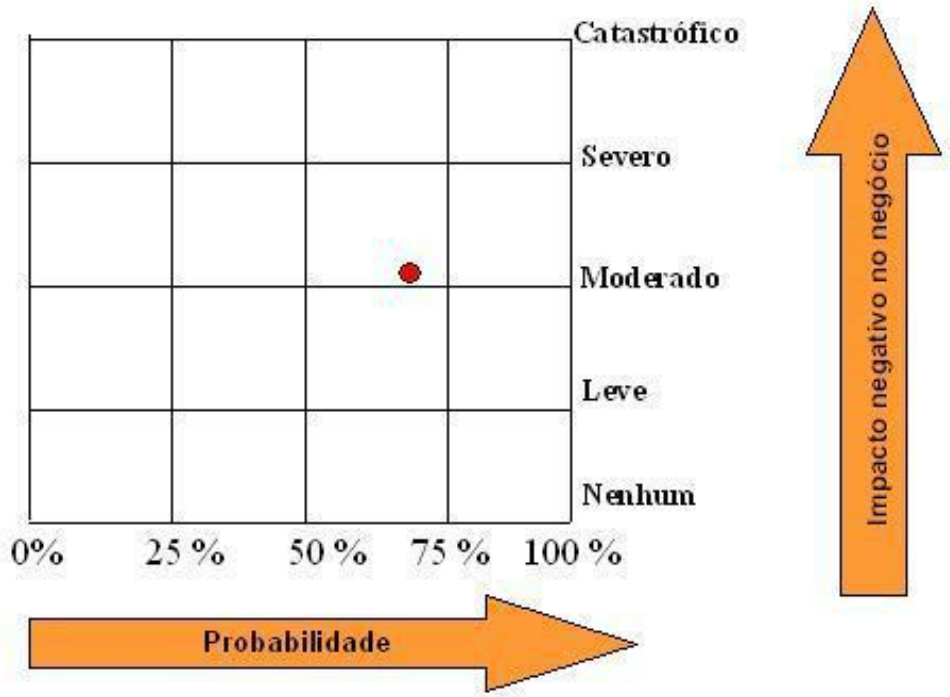
Elas se baseiam em duas premissas básicas que são:

A probabilidade da ocorrência;

O impacto financeiro para o negócio;

As matrizes podem ter estas formas:

**MATRIZ DE VULNERABILIDADE**



**MATRIZ DE SUPORTABILIDADE**

| | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | Frequente | Provável | Ocasional | Remota | improvável |
| | | Elevada | Alta | Média | Baixa | Muito baixa |
| IMPACTO | Catastrófico - I | Investimento Imediato | | | | |
| | Severo – II | | Monitoramento | | | |
| | Moderado – III | | | Contingência | | |
| | Leve - IV | | | Zona de conforto | | |

**Outro modelo é a Matriz de Aceitabilidade**:

**Frequência da Ameaça**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8 | Constante | | | | | | |
| 7 | Habitual | | | | | | |
| 6 | Frequente | | | | | | |
| 5 | Moderado | | | | | | |
| 4 | Ocasional | | | | | | |
| 3 | Esporádico | | | | | | |
| 2 | Remoto | | | | | | |
| 1 | Improvável | | | | | | |
| | | Insignificante | Marginal | Grave | Crítico | Desastroso | Catastrófico |
| | | 1 | 2 | 5 | 10 | 20 | 50 |

Consequência / Vulnerabilidade

Aceitável Tolerável Inaceitável Inadmissível

Seja qual for o método de análise de risco empregado ou a forma que a matriz se apresente, ela é uma ferramenta indispensável para o gestor, pois irá auxilia-lo na priorização das ações tendo em vista a probabilidade de ocorrência e o impacto que, caso o risco ocorra, trará para o negócio.

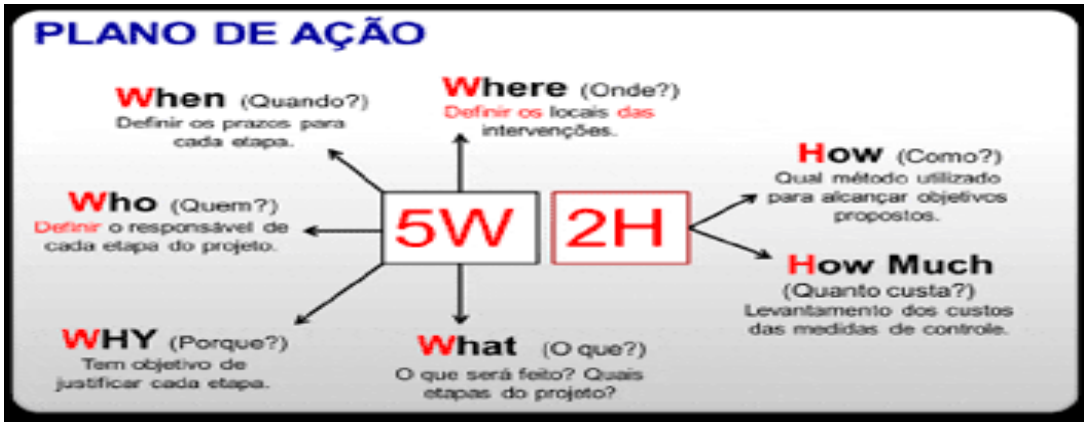
A matriz apresenta de forma clara, quais são as prioridades de tratamento que daremos aos riscos que a empresa apresenta. É uma forma de estabelecer a

priorização dos riscos a serem tratados de maneira clara e objetiva, atuando nos riscos que têm maiores prioridades de ocorrência e que trazem maiores impactos para a empresa.

Baseados nessas prioridades é que iremos elaborar nosso plano de ação.

Essas matrizes nós já publicamos, aqui, no Jornal da Segurança na edição nº 149.

No próximo mês daremos continuidade neste artigo, onde falaremos sobre o plano de ação e as formas de controle e avaliação da implantação deste plano.




# PLANEJAMENTO TÁTICO - ELABORAÇÃO DO PLANO DE AÇÃO

Em continuidade à matéria publicada na edição anterior sobre planejamento tático, utilizamos uma sequência prática para a elaboração do plano, que se apresenta em sete fases, das quais cinco etapas já foram analisadas na edição nº 165 (maio/08).

O plano de ação tem como objetivo determinar quais os recursos que a empresa empregará para mitigar os riscos relacionados. Na verdade, o plano deverá relacionar, de forma ordenada, quais as providências necessárias para diminuir a probabilidade e/ou o impacto da concretização do risco.

Essas ações já foram identificadas quando concluímos a segunda fase do planejamento, ou seja, a identificação dos fatores de risco.

Desse modo, tudo que foi relacionado no diagrama de causa e efeito e na matriz SWOT será inserido no plano de ação.

Além disso, levará em conta a classificação dos riscos que foram expostos nas matrizes de vulnerabilidade ou suportabilidade, que deverão determinar quais as prioridades da empresa.

Dessa maneira, o gestor poderá priorizar os riscos que têm maiores probabilidades de ocorrência e maior impacto em sua companhia.

O cruzamento destas variáveis – impacto e probabilidade - resulta na perda esperada, que determina qual o valor máximo a ser investido na mitigação dos riscos.

Sabendo disso, o plano de ação transforma toda a técnica aplicada à análise de risco em ação, em prática e em funcionamento, ou seja, é quem faz acontecer.

**5W2H**

Uma forma muito conhecida para a elaboração do plano de ação é a ferramenta de qualidade chamada 5W2H.

Esta sigla representa as palavras, em inglês, what (o que deve ser feito), who (quem é o responsável pela execução), where onde (setor/local em que deve ser executado), when quando (a ocasião em que deve ser executado – é importante definir uma data limite para a conclusão do trabalho) e why (porque deve ser executado, ou seja, qual a finalidade ou resultado esperado).

Já o 2H representa o how como (de que maneira deve ser executado - qual o método) e how much quanto custa (quanto será gasto para executar).

**PLANO DE AÇÃO**

| O QUE | QUEM | ONDE | QUANDO | POR QUE | COMO | QUANTO CUSTA |
|---|---|---|---|---|---|---|
| Compra e instalação de catracas | João | na portaria 03 | Até 30/12/08 | Controlar acesso de pessoas | Contratando empresa especializada | R$ 500 |
| Crachá em PVC | Pedro | na recepção | Até 30/12/08 | Identificar visitantes | Aquisição de material | R$ 300 mil |
| Treinamento dos vigilantes que trabalham na portaria 03 | Maria | na sala de treinamento do setor | Até 30/12/08 | Atender Procedimentos para emissão de crachá e controle de acesso de visitantes | Aos sábados das 08h às 12h. Demonstração do equipamento e explicação | R$ 100 |

**RELATÓRIO DE TRÊS GERAÇÕES**

Também podemos utilizar outra ferramenta que auxiliará no acompanhamento do plano de ação, chamada de relatório de três gerações, que possui esse nome porque observa os três tempos: passado, presente e futuro.

Deve observar o que foi planejado, executado, os resultados, os pontos problemáticos e como resolvê-los.

Esta ferramenta permitirá o acompanhamento do plano de ação, propondo correções, caso sejam necessárias.

O relatório de três gerações poderá ser representado da seguinte forma:

**RELATÓRIO DE TRÊS GERAÇÕES**

| PLANEJADO | EXECUTADO | RESULTADOS | PONTOS PROBLEMÁTICOS | PROPOSIÇÃO |
|---|---|---|---|---|
| Compra e instalação de catracas | O equipamento foi comprado, mas não foi instalado | Falta a instalação do equipamento | Falta infraestrutura elétrica adequada no local | Contratar empresa para instalação elétrica |
| Crachá em PVC | O material não foi comprado | Não há material para a confecção dos crachás | O produto teve aumento substancial de preço, ultrapassando o limite previsto | Importar o material com preços mais acessíveis |

Observação: este relatório é preenchido pelo responsável pela ação e não pelo coordenador do projeto.

Planejado

Nesta coluna são inseridas as contramedidas propostas no plano de ação.

Executado

Informações sobre o que foi realizado, pois nem sempre o que estava previsto (planejado) foi executado

Resultados

Aqui, as informações inseridas referem-se à meta proposta no plano de ação.

Pontos problemáticos

Causas e fatores que impediram que a meta fosse alcançada.

Proposição

Aqui são inseridas as contramedidas para cada causa, ou seja, quais as opções ou como o problema listado na coluna anterior será resolvido.

Controle e avaliação

Nesta fase, acompanharemos o andamento do projeto, ou seja, se o que foi planejado está sendo executado no tempo previsto e com os padrões preestabelecidos.

Controlar é acompanhar a evolução do projeto, confrontando o seu desempenho com padrões antes definidos.

Em caso de desvios, deve-se adotar medidas para corrigi-los (veja as fases do controle).

Seguindo as fases sequenciais apresentadas, podemos elaborar um plano tático de segurança, aplicável e estruturado de maneira técnica, aplicando-se ferramentas da administração científica e da qualidade, aqui adaptadas.

É claro que existem outras ferramentas que poderiam substituí-las e não estariam erradas.

No entanto, o objetivo foi mostrar uma sequência fácil, técnica e que apresenta resultados eficazes na segurança de empresas e condomínios, que podem ser úteis para os gestores e consultores de segurança e, principalmente, sair do “achismo”, infelizmente ainda tão presente no segmento.

**FASES DO CONTROLE**

Fixar metas e indicadores

Estabelecer padrões ou critérios.

Os padrões representam o desempenho desejado e são expressos em tempo, dinheiro, qualidade, unidades físicas, custos ou índices.

Comparar desempenho com metas e indicadores

Observar o desempenho.

Para se controlar o desempenho deve-se ao menos conhecer algo a respeito dele.

A observação ou verificação do desempenho ou resultado busca informações precisas sobre aquilo que está sendo controlado.

Providências para correção de desvios

Comparar o desempenho com o padrão estabelecido.

O desempenho deve ser comparado ao padrão para verificar eventuais desvios. É feito por meio de gráficos, relatórios, índices, porcentagens, medidas e estatísticas.

Tais meios de apresentação supõem técnicas à disposição do controle, para que este tenha mais informações sobre o que deverá ser controlado.

Ação corretiva

Manter as operações dentro dos padrões definidos para que os objetivos sejam alcançados. Os erros ou desvios devem ser corrigidos.

Estas ações podem ser sobre o sistema adotado, procedimentos, pessoas, desempenho específicos, entre outros.

1

# REFERÊNCIAS

## Artigos de Cláudio dos Santos Moretti - CES, ASE.


**Riscos globais para os próximos 10 anos.** Artigo publicado no Jornal da Segurança nº 248 de abril de 2015.

**Qual a importância da análise de risco para o profissional de segurança**. Artigo publicado na Revista PROTEGER nº 54 de maio de 2007 (atualizado).

**Gestão de risco, a nova norma da ABNT**. Artigo publicado no Jornal da Segurança nº 210 de fevereiro de 2012. (Atualizado)

**Qual a importância da gestão de risco no planejamento da segurança**. Artigo publicado na revista do SESVESP nº 113 de maio/junho 2013.

**A importância da gestão de risco no transporte de cargas**. Artigo publicado no Jornal da Segurança nº 194 de outubro de 2010.

**Gestão de risco – Identificação dos riscos e fatores de risco**. Artigo publicado no Jornal da Segurança nº 144 de agosto de 2006 (atualizado).

**Diagnóstico de Segurança**. Artigo publicado na Revista Gestão de Riscos nº 143 de abril/junho de 2020.

**Metodologia para análise de riscos – Método Estatístico**. Artigo publicado no Jornal da Segurança nº 145 de setembro de 2006 (ATUALIZADO).

**Métodos de análise de risco – Método Mosler**. Artigo publicado no Jornal da Segurança nº 146 de outubro de 2006 (atualizado).

**Método de análise de risco – T. Fine**. Artigo publicado no Jornal da Segurança nº 147 de novembro de 2006. (Atualizado).

**Método brasiliano (básico) para análise de riscos**. Artigo publicado no Jornal da Segurança nº 148 de dezembro de 2006. Adaptado.

**Planejamento Tático de Segurança**. Artigo publicado no Jornal da Segurança nº 165 de maio de 2008.

**Planejamento tático - Elaboração do plano de ação**. Artigo publicado no Jornal da Segurança nº 167 de julho de 2008.

**Planejamento de segurança e as normas de gestão de risco.** Artigo publicado no Jornal da Segurança nº 221 de janeiro de 2013 (atualizado).

**ISO 31000 – norma de gestão de riscos.** Artigo publicado no Jornal da Segurança nº 187 de maço de 2010.

## OUTRAS REFERÊNCIAS CITADAS

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos - gestão integrada em riscos corporativos.** São Paulo: Sicurezza, 2018.

_____, Antonio Celso Ribeiro. **Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado – ISO 31000.** São Paulo: Sicurezza, 2009.

_____, Antonio Celso Ribeiro. **Manual de Planejamento/ Gestão de Riscos corporativos.** São Paulo: Sicurezza, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC. **Gestão de Riscos – Princípios e diretrizes. NBR ISO 31000**. Associação Brasileira de Normas Técnicas. 2009.

_____, ABNT NBR ISO/IEC 31010: **Gestão de riscos: Técnicas para o processo de avaliação de riscos**. Rio de Janeiro, 2012.