GESTÃO DE RISCOS

Autoria: Antonio Celso Ribeiro Brasiliano

UNIASSELVI-PÓS

Programa de Pós-Graduação EAD

UNIASSELVI

CENTRO UNIVERSITÁRIO LEONARDO DA VINCI
Rodovia BR 470, Km 71, nº 1.040, Bairro Benedito
Cx. P. 191 - 89.130-000 – INDAIAL/SC
Fone Fax: (47) 3281-9000/3281-9090

Reitor: Prof. Hermínio Kloch

Diretor UNIASSELVI-PÓS: Prof. Carlos Fabiano Fistarol

Coordenador da Pós-Graduação EAD: Prof. Ivan Tesck

Equipe Multidisciplinar da
Pós-Graduação EAD: Prof.ª Bárbara Pricila Franz
Prof.ª Tathyane Lucas Simão
Prof. Ivan Tesck

Revisão de Conteúdo: Jorge Hilário Bertoldi
Revisão Gramatical: Equipe Produção de Materiais

Diagramação e Capa:
Centro Universitário Leonardo da Vinci – UNIASSELVI

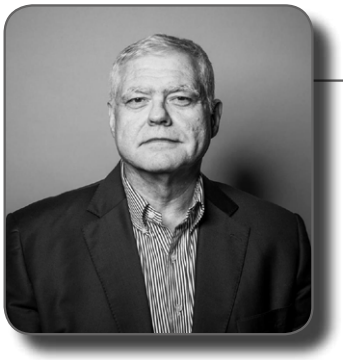
Ficha catalográfica elaborada na fonte pela Biblioteca Dante Alighieri
UNIASSELVI – Indaial.

22
B823g Brasiliano, Antônio Celso Ribeiro
Gestão de riscos / Antônio Celso Ribeiro Brasiliano. Indaial: UNIASSELVI, 2018.

147 p. : il.

ISBN 978-85-69910-85-5

1.Gestão Empresarial.
I. Centro Universitário Leonardo Da Vinci.



Dr. Antonio Celso Ribeiro Brasiliano

Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique (Ciência e Engenharia da Informação e Inteligência Estratégica) pela UNIVERSITÉ EAST PARIS - MARNE LA VALLÉE – Paris – França; Master Degree - Diplome D´Etudes Approfondies (DEA) en Information Scientifique et Technique Veille Technologique (Inteligência Competitiva) pela UNIVERSITE TOULON – Toulon - França; Especializado em: Inteligência Competitiva pela Universidade Federal do Rio de Janeiro - UFRJ; Gestión da Seguridad Empresarial Internacional – Universidad Pontifícia Comillas de Madrid – Espanha; Curso de Gestión da Seguridad Empresarial - Universidad Pontifícia Comillas de Madrid – Espanha; Planejamento Empresarial, pela Fundação Getúlio Vargas - SP; Elaboração de Currículos pelo Centro de Estudos de Pessoal do Exército - CEP, Bacharel em Ciências Militares, graduado pela Academia Militar das Agulhas Negras; Bacharel em Administração de Empresas – Universidad Mackenzie; Certification in Risk Management Assurance – CRMA, pelo IIA Global – Institute of Internal Auditors,Certificado como Especialista em Segurança Empresarial– CES pela ABSO. Autor dos livros: Inteligência em Riscos: Gestão Integrada em Riscos Corporativos; Gestão de Risco de Fraudes , Fraud Risk Assessment – FRA, "Gestão de Continuidade de Negócios – GCN"; Guia Prático para a Gestão de Continuidade de Negócios, Cenários Prospectivos em Gestão de Riscos Corporativos: um estudo de caso brasileiro; " Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado" – Alinhado com a ISO 31000; "Análise de Risco Corporativo – Método Brasiliano"; "Manual de Análise de Risco Para a Segurança Empresarial"; "Manual de Planejamento: Gestão de Riscos Corporativos"; "A (IN)Segurança nas Redes Empresarias: A Inteligência Competitiva e a Fuga Involuntária das Informações"; "Planejamento da Segurança Empresarial: Metodologia e Implantação"; Co-Autor dos Livros: "Dicionário de Crime, Justiça e Sociedade", lançamento em Portugal onde colaborou com especialistas portugueses e demais países da Europa, sendo o único brasileiro a participar com textos sobre Fraudes Corporativas; "Manual de Planejamento Tático e Técnico em Segurança Empresarial"; "Segurança de Executivos" - Noções Anti-Seqüestro e Seqüestro: Como se Defender; ; Idealizador da Solução em Inteligência em Riscos Corporativos INTERISK; Professor Convidado do IPT da USP do Programa de Mestrado, para aulas de Análise de Riscos, da Fundação Dom Cabral, da FIA - USP e da Faculdade Trevisan para Cursos de Gestão de Riscos, Atual Coordenador Técnico e Professor do MBA - Gestão de Riscos Corporativos e Cursos de Extensão nos temas de Riscos, Compliance, Gestão de Continuidade de Negócios, Auditoria Baseada em Riscos, Controles Internos, Segurança Corporativa, todos

em convênio com a Faculdade de Engenharia de São Paulo – FESP; Membro do Institute of Internal Auditors IIA; do Instituto dos Auditores Internos do Brasil – IIA Brasil; Membro da Associação Brasileira de Profissionais de Segurança Orgânica – ABSO, Coordenou a 1ª Pesquisa de Vitimização Empresarial 2003 – Contrato pela PENUD/ONU/SENASP; Profissional com mais de 25 anos de experiência em Gestão de Riscos, Palestrante nacional em inúmeros eventos da área de riscos, compliance, auditoria, controles internos e segurança corporativa. Palestrante Internacional em eventos na Argentina, Paraguai, África e Japão (convidado pelo Organização PanAmericana de Saúde-OPAS, como expert em Planos de Contingência, na Conferência Mundial de Redução de Desastres,Yokohama). Experiência internacional em consultoria GRC em Portugal, Cabo Verde, Angola, Moçambique, Uruguai, Argentina, Paraguai, Colômbia, México. Membro da Comissão de Estudo Especial de Gestão de Riscos da ABNT/CEE-63 – ISO 31000/31010/31004 – Gestão de Riscos e ISO 22301/22313 Gestão de Continuidade de Negócio – Segurança da Sociedade. É Presidente da BRASILIANO INTERISK GESTÃO DE RISCOS.

Sumário

APRESENTAÇÃO

Prezados pós-graduandos (as), vocês possuem, neste material didático, o livro de Gestão de Riscos do seu curso.

As instituições, públicas e ou privadas, devem estar comprometidas com seus clientes internos e a sociedade, focando esforços em reduzir os riscos existentes em seus processos visando maximizar as oportunidades e ganhos de produtividade. Para tanto, é necessário conhecer os riscos que afetam os seus processos, bem como seus respectivos impactos.

Os riscos permeiam todos os níveis dos processos e, se não forem gerenciados adequadamente, poderão resultar em perdas financeiras, deterioração da imagem e reputação ou desencadear uma crise.

O gerenciamento de riscos tem se tornado um assunto de suma importância em qualquer meio, uma vez que a conscientização da necessidade de administração dos riscos potenciais é, hoje, uma questão de sobrevivência e produtividade. Para que seja eficaz, o gerenciamento de riscos deve fazer parte da cultura de qualquer instituição e deve estar inserido em sua filosofia, nas práticas e nos processos operacionais, estratégicos e administrativos.

Neste sentido, este livro é essencial para que vocês possam identificar riscos nos processos que já estão desenhados, e naqueles que vierem a ser mapeados. Os riscos são compostos por fatores de riscos ou fontes de riscos, tanto internas como externas, aos processos, chamadas de causas. Estas causas são, na verdade, as fragilidades que os processos possuem, tais como: ausência de segregação de função, falta de checagem de determinados documentos e assim por diante. Diante das fragilidades dos processos é que são implantados os controles, considerados como medidas preventivas para diminuir as chances dos riscos virem a se materializar, e também as medidas mitigatórias visando diminuir os impactos.

Os controles que vocês implantaram nos processos devem ser bem pensados, com base na relação custo *versus* benefício. Daí a importância estratégica deste livro, pois ele está fornecendo para vocês ferramentas de decisão em análise de risco.

A análise de risco demonstra de forma clara e transparente o grau de risco que o processo está exposto, frente à probabilidade de ocorrência - chance do risco materializar-se, de acordo com as condições operacionais do processo e suas consequências financeiras, legais, operacionais e de imagem da organização. Desta forma, temos com estes dois critérios chamados de

probabilidade e impacto, a criticidade dos riscos, plotado em uma Matriz de Risco. Com esta visão na Matriz de Risco podemos tomar a decisão sobre quais fases do processo necessitam de controles, visando tornar o processo ágil, flexível e ao mesmo tempo seguro, dentro do apetite ao risco da organização.

Este livro de Gestão de Riscos em Processos possui uma metodologia que integra as variadas disciplinas de riscos, todas debaixo do mesmo *Framework*, falando a mesma linguagem, de tal forma que possa haver uma interpretação das informações relevantes gerando a verdadeira Inteligência em Riscos para a organização. Esta Inteligência em Riscos agrega valor para os processos e previne as incertezas do ambiente, ajudando você a priorizar recursos.

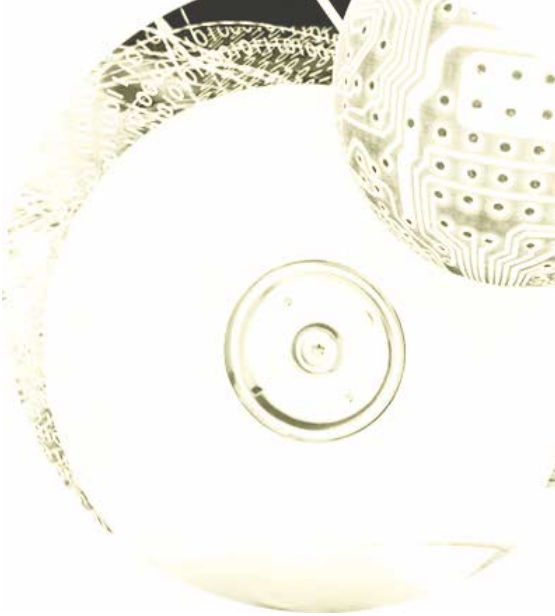
Você encontrará também, técnicas de Gestão de Riscos alinhadas e integradas com as três melhores práticas de mercado: ISO 31000, o COSO I Controles Internos, revisado em 2013 e COSO II - Gestão Integrada de Riscos. O motivo da integração das três estruturas em um só *framework* é que o contexto passa por fortes mudanças, exigindo dos gestores e da administração um modelo de Gestão de Riscos flexível, mas ao mesmo tempo consistente e estruturado para atender as regulações e exigências do mercado.

Encerro a apresentação deste material didático pedindo a vocês pós-graduandos (as), que façam uma reflexão nas palavras do explorador da Antártica Norman Vaughan, quando tiverem dificuldade em colocar em prática o processo ou encontrar resistência de seus pares ou superiores:

“Dream Big and Dare to Fail, podemos fazer a versão para o português em *“Sonhe grande e ouse fracassar.”.*

Recado: Não tenhamos medo neste mundo de incerteza, se temos convicção, vamos em frente!!

Sucesso a todos!



Capítulo 1

Contexto e Gestão de Riscos Corporativos

A partir da perspectiva do saber fazer, neste capítulo você terá os seguintes objetivos de aprendizagem:

- ✓ Compreender a concepção do conceito VUCA em inglês, VICA em português, nos ambientes e situações de negócio.
- ✓ Analisar a importância de todos os gestores saberem lidar com as incertezas, através de cenários complexos e altamente dinâmicos.
- ✓ Compreender a origem da Gestão de Riscos.
- ✓ Analisar os conceitos e abrangência do Gerenciamento de Riscos.
- ✓ Analisar a nova função do Gerenciamento de Riscos Corporativos, destacando a necessidade da Inteligência em Riscos.
- ✓ Compreender a concepção das Três Linhas de Defesa.
- ✓ Analisar a abrangência e aplicação das Três Linhas de Defesa, dentro da Governança da organização.

Contextualização

Este capítulo visa abordar que o mundo vive em uma velocidade muito grande. Para tanto, inicialmente vamos estudar a concepção do conceito VUCA em inglês, VICA em português, que reforça a complexidade da nossa sociedade contemporânea, devido à interdependência e a globalização. Por esta razão é que a Gestão de Riscos deve ser internalizada nas organizações.

Aborda que o Gerenciamento de Riscos Corporativos orienta seu enfoque diretamente para o cumprimento dos objetivos estabelecidos por uma organização e fornece parâmetros para definir a eficácia desse gerenciamento de riscos. Dessa forma a administração das organizações devem ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e estratégicas. Para este fim, é necessária a criação de uma área específica, com uma estrutura e recursos definidos.

Além disso, apresentamos os conceitos e abrangência da Três Linhas de Defesa, destacando papéis e responsabilidades adequadas à Governança da organização.

Mercado - Características

Hoje o mercado passa pelo que chamamos pelo anacrônico VUCA, uma sigla utilizada para descrever a volatilidade (volatility), a incerteza (uncertainty), a complexidade (complexity) e a ambiguidade (ambiguity) nos ambientes e situações de negócio.

Hoje o mercado passa pelo que chamamos pelo anacrônico VUCA, uma sigla utilizada para descrever a volatilidade (volatility), a incerteza (uncertainty), a complexidade (complexity) e a ambiguidade (ambiguity) nos ambientes e situações de negócio.

VUCA em inglês, VICA em português é oriundo do vocabulário militar americano. O uso comum do termo VUCA começou no final dos anos 1990. O conceito VUCA expressa a complexidade da nossa sociedade contemporânea, devido à interdependência e a globalização, situações que antes tinham pouco impacto, mas que agora refletem em toda sociedade, por exemplo, a catástrofe de Fukushima, em 2011, fez as montadoras japonesas no Brasil pararem suas linhas produtivas devido à falta de peças, ou seja, a interdependência é uma realidade no mundo globalizado e deve fazer parte da gestão de riscos.

Partindo desta abordagem, o *US Army War College* formulou um programa de formação para o desenvolvimento das lideranças militares, ao nível estratégico, o qual contempla a adoção de metodologias adequadas para enfrentar o VUCA e fazer frente a um ambiente extremamente agressivo e predador. O *US Army College*, caracteriza os componentes deste contexto envolvente do seguinte modo:

- **Volatilidade:** É marcada pelo ritmo elevado com que ocorrem mudanças com impacto na vida das sociedades desenvolvidas e, concomitantemente, nas suas organizações. Assim, no atual contexto de uma Era da Informação e do Conhecimento, os dados e as evidências existentes no momento presente podem não ser suficientes para a tomada de decisão. Antecipar e prever o que pode acontecer, por exemplo, durante o período de execução de um projeto, são dimensões, por vezes, absolutamente decisivas.

- **Incerteza:** É uma característica do contexto marcada pela necessidade de se assumir que o conhecimento sobre uma dada situação é sempre incompleto, potencializando, deste modo, o aparecimento de opiniões divergentes sobre a melhor estratégia a prosseguir, exigindo uma cuidadosa análise do risco. De fato, é cada vez mais difícil levantar cenários futuros com base em acontecimentos passados.

- **Complexidade:** Característica do contexto envolvente que está associada à dificuldade de compreender o resultado das interações das várias componentes de um sistema, uma vez que estas raramente são de natureza mecanicista e linear. A Teoria da Complexidade vem, deste modo, mostrar a interdependência essencial de todos os fenômenos. Neste ponto, a assunção de fenômenos complexos, no seio de uma organização, impõe a necessidade de admitir interações não-lineares entre os componentes do sistema, com consequências que se multiplicam rápida e imprevisivelmente. Característica mais marcante do século XX e XXI!

- **Ambiguidade:** Descreve um tipo específico de incerteza que resulta de diferenças na interpretação quando as evidências existentes são insuficientes para esclarecer o significado de um determinado fenômeno. Na prática, no âmbito da gestão das organizações, a consequência deste fato é a elevada probabilidade das lideranças poderem interpretar, legitimamente, eventos de formas diferentes, aumentando significativamente a probabilidade de erros na interpretação dos mesmos. A imprecisão da realidade, o potencial de erros de leitura, os significados mistos de condições; a falta de ação, confusão entre causa e efeito e a falta de clareza. Para HUTCHINS (2011), especialista americano em gestão da qualidade e gestão de risco: “nós estamos saindo de um mundo linear de saber a solução dos problemas e tomar uma decisão clara para um mundo dinâmico de entender o sentido, de tomada de decisão baseada no risco, em condições VUCA”.

O mundo VICA só pode ser gerenciado com base em riscos. Daí a importância de todos os gestores saberem a competência de lidar com as incertezas. O mundo VICA é baseada na própria gestão de riscos, lidando com cenários complexos e altamente dinâmicos, onde se exige dos gestores:

O mundo VICA só pode ser gerenciado com base em riscos. Daí a importância de todos os gestores saberem a competência de lidar com as incertezas. O mundo VICA é baseada na própria gestão de riscos, lidando com cenários complexos e altamente dinâmicos, onde se exige dos gestores:

- **Visão do todo e não da parte**: O gestor tem que enxergar a floresta e não a árvore;
- **Grande velocidade na tomada de decisão**: O movimento é mais importante, não podemos ficar parados, se ficarmos o inimigo mata! O ótimo é inimigo do bom, conhecem?;
- **Não ortodoxia**: Pensar fora da caixa, não dogmatizar soluções, ser criativo diante das incertezas;
- **Colaboração e co-criação entre as equipes**: Redes de colaboração, estar conectado para o entendimento rápido do contexto;
- **Agilidade**: Saber mover-se com grande flexibilidade, possuir estrutura leve para poder carregar.

Atividades de Estudos:

1) O que significa a sigla VICA?

_____
_____
_____
_____

2) Para que os gestores possam lidar com as incertezas, qual as competências que eles precisam possuir?

_____
_____
_____
_____

Origem da Gestão de Riscos

A origem da gerência de risco teve seu início efetivo nos Estados Unidos e em alguns países da Europa, logo após a segunda Guerra Mundial, começando a reduzir os gastos e aumentar a proteção da empresa, frente aos riscos reais e potenciais.

A origem da gerência de risco teve seu início efetivo nos Estados Unidos e em alguns países da Europa, logo após a segunda Guerra Mundial, tendo os responsáveis pela segurança das grandes empresas, bem como, os responsáveis pelos seguros, começando a examinar a possibilidade de reduzir os gastos com prêmios de seguro e aumentar a proteção da empresa, frente aos riscos reais e potenciais. Só seria possível atingir tais objetivos e redução dos custos, com uma profunda análise das situações de risco.

Além da avaliação das probabilidades de perda, tornou-se necessário identificar quais riscos poderiam ser considerados inevitáveis e quais poderiam ter a chance de concretização diminuída de forma direta. Em cima deste estudo detalhado, levantou-se a relação custo x benefício das medidas de segurança a serem implantadas, bem como, a situação financeira da empresa, para escolha adequada do nível de segurança a ser atingido.

A partir da década de 70, o gerenciamento de riscos ligado à área de crédito e financeiro, tomou uma proporção grande, tendo em vista os sinais dos tempos de mudança.

A partir da década de 70, o gerenciamento de riscos ligado à área de crédito e financeiro, tomou uma proporção grande, tendo em vista os sinais dos tempos de mudança. A desregulamentação, a globalização e a desintermediação mudaram a definição dos mercados e alteraram os aspectos econômicos das operações desses mercados.

Uma pesquisa recente, realizada pela British Bankers Association (BBA), levantou que 70% dos bancos do Reino Unido consideravam seus riscos operacionais tão importantes quanto os riscos de crédito e de mercado. Quase um quarto daqueles bancos havia experimentado perdas relacionadas a operações de US$ 1,6 milhões de dólares. Dados históricos de perdas da Operational Risk Inc (ORI) sugerem que em mais de 50 casos, instituições individuais perderam mais de US$ 500 milhões cada uma, enquanto que, em 30 casos, empresas perderam acima de US$ 1 bilhão cada uma.

Os acontecimentos em 2001, desde o ataque terrorista até as grandes fraudes nas corporações americanas, e, em 2015 no Brasil, os casos de fraudes e corrupção, passaram a sensibilizar os decisores quanto à necessidade de monitorar, de forma constante, as variáveis internas e externas às organizações. Variáveis estas que podem influenciar sua Cadeia de Valor.

Definição de Gerenciamento de Riscos Corporativos

A gestão de riscos corporativos trata riscos e oportunidades que afetam a criação ou a preservação de valor. O processo de gestão de riscos corporativos deve ser efetivado de forma descentralizada, por todos os membros da organização. Portanto uma definição mais utilizada no mercado é a descrita no COSO II (2004, p. 4):

A gestão de riscos corporativos trata riscos e oportunidades que afetam a criação ou a preservação de valor.

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

O COSO II (2004, p. 4) reflete certos conceitos fundamentais:

1) É um processo contínuo e que flui através da organização como um todo;
2) É conduzido pelos profissionais em todos os níveis da organização, ou seja, é um processo descentralizado;
3) É aplicado à definição das estratégias, alinhado com seus objetivos estratégicos;
4) É aplicado em toda a organização, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta;
5) É formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a organização, e para administrar os riscos de acordo com seu apetite a risco;
6) É capaz de propiciar garantia razoável para o conselho de administração e a diretoria executiva de uma organização do cumprimento de seus objetivos, pois seus riscos estão gerenciados;
7) É orientado para a realização de objetivos em uma ou mais categorias distintas, mas dependentes.

Essa definição é intencionalmente ampla e adota conceitos fundamentais sobre a forma como as empresas e outras organizações administram riscos, possibilitando uma base para sua aplicação em organizações, indústrias e setores. O gerenciamento de riscos corporativos orienta seu enfoque diretamente para o cumprimento dos objetivos estabelecidos por uma organização específica e fornece parâmetros para definir a eficácia desse gerenciamento de riscos.

A Nova Função do Gerenciamento de Riscos Corporativos - Inteligência em Riscos

Cabe definirmos a Gerência de Risco, sob o aspecto do seguro, onde quase tudo começou sendo um processo para conservar o poder de ganho e o patrimônio da empresa (ou pessoa) pela minimização do efeito financeiro de perdas acidentais.

É preciso, também, estabelecer a distinção entre risco puro e risco especulativo. Os vários autores e estudiosos, principalmente norte-americanos, da Gerência de Riscos, digamos, "tradicional", têm classificado os riscos que podem atingir uma empresa, basicamente, em riscos especulativos (ou dinâmicos) e riscos puros (ou estáticos).

A diferença principal entre essas duas categorias reside no fato de que os riscos especulativos envolvem uma chance de ganho ou uma mesma possibilidade de perda, ao passo que os riscos puros envolvem somente uma possibilidade de perda, não existindo nenhuma chance de ganho ou de lucro.

Um exemplo clássico que mostra essa diferença é o do proprietário de um veículo, cujo risco (puro) que está associado a ele é o da perda potencial por colisão. Se eventualmente ocorrer uma colisão, o proprietário sofrerá, no mínimo, uma perda financeira. Se não ocorrer nenhuma colisão, o proprietário não terá, obviamente, nenhum ganho.

Hoje em dia a visão e o escopo do gerenciamento de risco corporativo ficou muito mais amplo, muito mais holístico, abrangendo inúmeras disciplinas nas empresas, decorrentes das atividades desenvolvidas nas organizações.

Hoje em dia a visão e o escopo do gerenciamento de risco corporativo ficou muito mais amplo, muito mais holístico, abrangendo inúmeras disciplinas nas empresas, decorrentes das atividades desenvolvidas nas organizações. A administração das instituições deve ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e estratégicas. Para este fim, é necessária a criação de uma área específica, com uma estrutura e recursos definidos.

As atividades de um departamento de gerenciamento de riscos corporativos, dentro do enfoque moderno, abrange inúmeras disciplinas. Muitas dessas atividades são comuns a uma ampla gama de funções administrativas. Por esta razão, é que este departamento deve possuir processo sistêmico e contínuo de identificação de exposição, medição, análise, controle, prevenção, redução, avaliação e financiamento de riscos. Esta nova função ajuda a integrar riscos financeiros e não financeiros tradicionais a

seguros e responsabilidade legal. É uma área que possui uma grande abrangência, mas com muitas interações através de diferentes disciplinas e, portanto, com uma necessidade de uma abordagem integrada. Algumas das disciplinas de riscos que devem se interagir são:

1) Riscos estratégicos
2) Riscos operacionais - ligados a operação
3) Riscos nos processos
4) Riscos de tecnologia da informação
5) Riscos de meio ambiente
6) Riscos de saúde e segurança do trabalho
7) Riscos de segurança empresarial
8) Riscos financeiros
9) Riscos legais
10) Riscos sociais
11) Riscos de sustentabilidade
12) Riscos de comunicação
13) Riscos de fraudes
14) Riscos na cadeia logística
15) Riscos no projeto
16) Outras tantas disciplinas

Estas disciplinas devem estar integradas com um único *Framework* e com Políticas integradas, visando a empresa falar uma mesma linguagem. Este é o principal desafio das empresas, integrar as disciplinas para que possam possuir a chamada Inteligência em Riscos Corporativos - IRC.

O gerenciamento de riscos, sob este enfoque, contribui para o fortalecimento e eficácia operacional e financeira da empresa, na medida que proporciona mecanismos de alocação de recursos para o seu emprego mais eficiente e eficaz, atingindo de forma direta a efetividade.

Portanto, a função do gestor de riscos é de integrar disciplinas e gerenciar as informações das inúmeras disciplinas de riscos. O gestor de riscos tem que relacionar os diversos riscos e verificar as interdependências entre eles. Hoje, por si só, não existe mais a possibilidade de só ter como ferramenta de gestão a Matriz de Riscos, mas deve também ter a Matriz de Impactos Cruzados para ver a motricidade entre riscos. Segundo o Fórum Econômico Mundial, em seu Relatório de Riscos Globais de 2017 ressalta: “A edição 2017 do relatório de Riscos Globais completa uma década destacando os riscos a longo prazo mais significantes ao redor do mundo, extraindo as perspectivas de especialistas e dos tomadores de decisões globais. Nesse tempo, a análise mudou da identificação dos riscos a pensar através das interconexões dos riscos e os potenciais efeitos-cascata que resultarão deles”.

Podemos então afirmar que a função do gestor de riscos corporativos é possuir Inteligência em Riscos, levando para a alta administração e/ou alto comando, os riscos considerados mais críticos, já com as conexões feitas. A figura a seguir mostra um modelo de gestão.

Figura 1 - Inteligência em Riscos - Função do Gestor de Riscos

A aréa de GRC como integradora e analista das informações estratégicas de riscos corporativos.

Fonte: Brasiliano (2016, p. 20).

Com o modelo anterior entendemos a Inteligência em Riscos em integrar soluções e indicadores, fornecendo para os decisores a visão holística dos riscos considerados críticos e as respectivas soluções integradas, com um farol de monitoramento de acompanhamento das evoluções. Desta forma a instituição possuirá, verdadeiramente, condições operacionais de se antecipar de forma objetiva a possíveis riscos, trabalhando de forma preventiva e não só de forma reativa. Com isso a organização ganha velocidade e competitividade, fatores chaves de sucesso em um mundo VICA!

Atividades de Estudos:

1) O que é gerenciamento de riscos corporativos, segundo o COSO?

_____
_____
_____
_____
_____
_____
_____

2) Qual é o objetivo de uma empresa implantar a Gestão de Riscos Corporativo?

a) Processo para certificação
b) Processo de antecipação, foco preventivo e mitigatório
c) Processo para melhoria da comunicação
d) Todas as alternativas acima estão corretas

3) No processo de gestão de riscos corporativos todas as disciplinas deverão:

a) possuir um único framework para padronizar o processo
b) cada disciplina deverá ter seu framework, em função da especificidade
c) as disciplinas não podem ter um único processo em função da complexidade
d) todas as alternativas acima estão erradas

Modelo das Três Linhas de Defesa

Uma das ferramentas adequadas à Governança Corporativa, foi lançada em 21 de setembro de 2010 pela FERMA - Federação das Associações Europeias de Gestão de Riscos, e pelo ECIIA - Confederação Europeia do Instituto de Auditoria Interna, é a Orientação sobre a 8ª Diretriz Jurídica Europeia da Empresa (Art. 41), que recomenda a utilização deste modelo de governança com o objetivo de definir responsabilidades entre as partes e o fluxo de comunicação e operacional, entre o conselho, a gestão, os executores de processos, os auditores, controles internos e gestão de riscos. O objetivo do documento foi o de auxiliar a gestão sênior na implementação da gestão de riscos, controle interno, *compliance* e auditoria interna e as relações com a diretoria executiva e conselho. O documento estabelece claramente as responsabilidades entre as áreas e suas relações. O conselho é responsável pela fiscalização da gestão de riscos da empresa e pelo framework de controle. Todos na empresa desempenham uma função na gestão eficaz de riscos, mas a responsabilidade primária para a gestão e o controle dos riscos é delegada ao nível de gestão adequado dentro da empresa. Ou seja, o processo é descentralizado e o dono do processo é o dono do risco. O CEO e o CFO possuem a responsabilidade final, perante o conselho, de todos os riscos e

controles. Para cumprir essas tarefas eficientemente, eles buscam se assegurar de várias fontes dentro da organização. O FERMA e o ECIIA apoiam o modelo das "três linhas de defesa" como um ponto de partida para a orientação regulatória futura. O modelo abaixo é o original publicado.

Figura 2 - Três Linhas de Defesa

Fonte: Ferma e ECIIA - Oitava Diretiva Européia.

Esta melhor prática foi concebida para descentralizar o procresso de controle

Esta melhor prática foi concebida para descentralizar o procresso de controle, dando aos usuários dos processos operacionais e estratégicos a responsabilidade primária de realizar o respectivo controle, com uma supervisão de áreas corporativas e da auditoria interna, de tal forma que haja cobertura em todos os níveis da empresa.

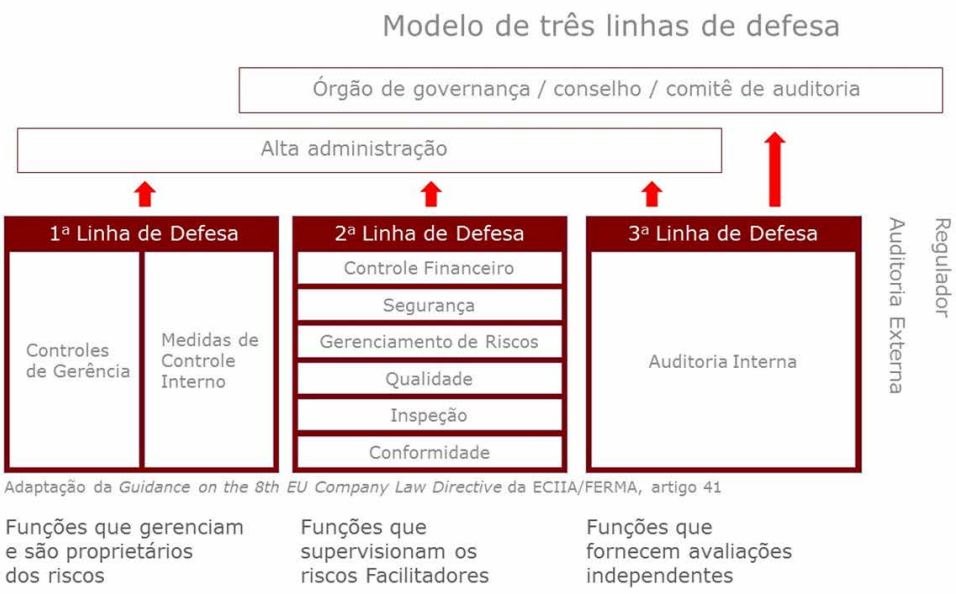
Com o crescimento significativo da complexidade no ambiente de negócios, as organizações passaram a necessitar de diferentes equipes de especialistas em controle interno, executivos de *compliance,* especialistas em gerenciamento de riscos, auditores internos, entre outros, para gerenciar, em conjunto e de forma efetiva seus principais riscos. Deve-se ressaltar, entretanto, que a divisão das atividades relacionadas ao gerenciamento de riscos entre diversos departamentos pode levar à ineficácia de algumas das ações promovidas. Assim, passa a ser fortemente recomendável que os esforços empreendidos por todos sejam devidamente coordenados, de modo a garantir que os processos sejam conduzidos de acordo com o que foi planejado. Conforme com o modelo apresentado, o conselho de administração e o diretor executivo, em nome da alta administração, são responsáveis pela supervisão e monitoramento dos processos de gestão de riscos e, para assumir de forma efetiva essas atribuições, eles necessitam de resultados provenientes das várias áreas envolvidas com este assunto. Esse modelo ganhou rapidamente um reconhecimento mundial por parte

das organizações e das entidades que representam as funções de gerenciamento de riscos e controles e, a partir de 2013, passou a ser divulgado também através de uma Declaração de Posicionamento do IIA – The Institute of Internal Auditors.

O controle da gerência é a primeira linha de defesa no gerenciamento de riscos

No modelo de Três Linhas de Defesa, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa e a avaliação independente é a terceira. Cada uma dessas três "linhas" desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

Figura 3 - Três Linhas de Defesa - Modelo IIA



Fonte: Declaração de Posicionamento do IIA - The Institute of Internal Auditors.

Este modelo reforça de forma incisiva que o dono do processo é o dono do risco e de seus controles. Portanto, os riscos corporativos só acontecem quando os donos do processo não possuem comprometimento e maturidade de praticarem os controles e respectivas metodologias, sugeridas e supervisionas pela segunda linha de defesa. A segunda linha de defesa é, na verdade, o grande guardião do processo, pois incentiva que a primeira linha pratique e ao mesmo tempo supervisiona para identificar possíveis falhas. A terceira linha, Auditoria Interna, realiza suas avaliações tanto na primeira como na segunda linha de defesa.

O processo das 3 linhas de defesa reforça o que já escrevi na definição da área de Gestão de Riscos, que deve haver Inteligência em Riscos Corporativos - IRC. Esta inteligência só poderá ser alcançada se adotar a prática de o dono do processo ser dono do risco. O dono do processo ser o responsável em realizar a auto-avaliação dos riscos e controles. Com este processo rodando, a segunda linha de defesa pode fazer seu papel estratégico de interpretar e de realizar os estudos de interconectividade entre riscos, entre áreas e entre processos. A auditoria interna por sua vez, utilizará como insumo as informações, tanto da segunda linha como da primeira, para realizar seus testes de controles, em processos críticos/chaves.

Atividades de Estudos:

1) De acordo com as três linhas de defesa, a essência do conceito pode ser resumido com a premissa:
Assinale V para as sentenças verdadeiras e F para as falsas.

( ) Os donos do processo são proprietários dos riscos, ou seja, as médias gerências
( ) A gerência de riscos é a proprietária dos riscos, sendo responsável em fazer a análise e gestão dos riscos.
( ) A auditoria é a responsável em fiscalizar, de forma independente, o processo de gestão de riscos.

Assinale a alternativa correta:

a) V – F – V.
b) V – V – V.
c) F – V – V.
d) V – V – F.

Algumas Considerações

O mundo VICA é um mundo que, para ser vencido, é preciso possuir preceitos da Gestão de Riscos. Por esta razão é que a Gestão de Riscos deve ser internalizada nas organizações de forma a possuir capilaridade em todos os processos e respectivos níveis organizacionais. Com isto a média e alta gerência das organizações estarão aptas a lidarem com o mundo VICA.

O gerenciamento de riscos, contribui para o fortalecimento e eficácia operacional e financeira da organização, na medida que proporciona mecanismos de alocação de recursos para o seu emprego mais eficiente e eficaz, atingindo de forma direta a efetividade.

Num cenário onde as mudanças são velozes, as instabilidades permanentes e há um predomínio de alta imprevisibilidade, a formulação de estratégias organizacionais já não podem combinar com métodos tradicionais de projeção e análise. Mais uma vez o mundo VICA comparece integrado com a gestão de riscos, visando gerenciar a incerteza.

O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Hoje em dia a visão e o escopo do gerenciamento de risco corporativo ficou muito mais amplo, muito mais holístico, abrangendo inúmeras disciplinas nas empresas, decorrentes das atividades desenvolvidas nas organizações. A administração das instituições deve ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e ou estratégicas. Para este fim, é necessária a criação de uma área específica, com uma estrutura e recursos definidos.

As atividades de um departamento de gerenciamento de riscos corporativos, dentro do enfoque moderno, abrange inúmeras disciplinas. Estas disciplinas devem estar integradas com um único *Framework* e com Políticas integradas, visando a empresa falar uma mesma linguagem. Este é o principal desafio das organizações, integrar as disciplinas para que possam possuir a chamada Inteligência em Riscos Corporativos - IRC.

Portanto, a função do gestor de riscos é de integrar disciplinas e gerenciar as informações das inúmeras disciplinas de riscos. O gestor de riscos tem que

relacionar os diversos riscos e verificar as interdependências entre eles. Dessa forma a administração das organizações deve ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e estratégicas.

No modelo de Três Linhas de Defesa, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa e a avaliação independente é a terceira. Cada uma dessas três “linhas” desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

As três linhas deveriam existir, de alguma forma, em todas as organizações, não importando tamanho ou complexidade. O gerenciamento de riscos, normalmente, é mais sólido quando há três linhas de defesa separadas e claramente identificadas.

Referências

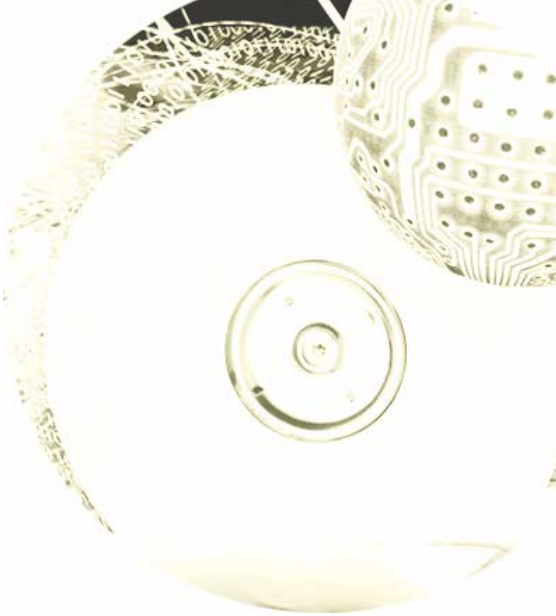
BRASILIANO, Antonio Celso Ribeiro. **Inteligência em Riscos**: Gestão Integrada em Corporativos. São Paulo: Editora Sicurezza, 2016.

COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management, 2004.

DECLARAÇÃO de Posicionamento do IIA - Instituto dos Auditores Internos: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.

FÓRUM Econômico Mundial, **Relatório de Riscos Globais**, 2017.

HUTCHINS, Greg. **Risk Management**: The Future of Quality, 2011.



Capítulo 2

Categorias de Riscos e sua Interconectividade

A partir da perspectiva do saber fazer, neste capítulo você terá os seguintes objetivos de aprendizagem:

- ✓ Compreender a concepção da Categoria de Riscos.
- ✓ Analisar a abrangência e aplicação da Categoria de Riscos.
- ✓ Compreender a concepção da natureza sistêmica dos Riscos, através da chamada Interconectividade ente Riscos.
- ✓ Analisar a abrangência e aplicação da Interconectividade entre Riscos.

Contextualização

Este capítulo visa abordar os conceitos e abrangência da Interconectividade entre Riscos, destacando a integração de Criticidade (Matriz de Riscos) versus Motricidade (Matriz de Impactos Cruzados), com o objetivo de obter uma visão estratégica de antecipação dos riscos.

Além disso, serão abordados os conceitos e abrangência da Categoria de Riscos, destacando que apesar da existência de referências, a Categoria de Riscos pode variar de acordo como segmento.

Categoria de Riscos

Não há uma fórmula para classificar riscos. Não existe uma classificação de riscos que seja consensual, exaustiva e aplicável a todas as organizações. A classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da indústria, mercado e setor de atuação.

A classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da indústria, mercado e setor de atuação.

Por exemplo: Os estoques de materiais de consumo são menos relevantes para um banco do que para uma indústria, onde pode representar um dos principais fatores de risco. Analogamente, as variáveis relacionadas ao “risco de mercado” são cruciais para um banco e podem não ser tão relevantes para determinada organização manufatureira.

Portanto, dependendo do tipo de segmento que a empresa atua podemos ter as seguintes categorias de riscos:

a) Risco Operacional

O risco operacional pode ser definido como uma medida numérica da incerteza dos retornos de uma instituição, caso seus sistemas, práticas e medidas de controle não sejam capazes de resistir a falhas humanas, danos à infraestrutura de suporte, utilização indevida de modelos matemáticos ou produtos, alterações no ambiente dos negócios, ou a situações adversas de mercado.

b) Risco Legal

O risco legal pode ser definido como uma medida numérica da incerteza dos retornos de uma instituição, caso seus contratos não possam ser legalmente amparados por falta de representatividade por parte de um negociador, por documentação insuficiente, insolvência ou ilegalidade.

c) Riscos Estratégico

O risco estratégico alveja um ou mais elementos cruciais na concepção do modelo de negócio da empresa, ou seja, afeta as atividades primárias da Cadeia de Valor. Em alguns casos podem até acabar com o vínculo da empresa com o mercado. Em outros casos, diminuem a proposta de valor que a empresa oferece, que pode ser a base do fluxo de receita. Podem também diluir os lucros dos quais dependem. Às vezes destroem a gestão estratégica que ajuda a empresa a monitorar e controlar a concorrência. No pior cenário possível, riscos estratégicos podem ameaçar todos os pilares que sustentam os objetivos da empresa.

No contexto moderno seguindo a citação de SLYWOTZKY e WEBER (2007), há sete grandes tipos de riscos estratégicos que qualquer empresa deve estar preparada para enfrentar. Embora a empresa vá continuar enfrentando outros tipos de riscos, dos tipos geopolítico, regulatório, operacional, esses setes riscos estratégicos compreendem a gama de riscos que expõe a concepção do negócio da maioria das empresas, ou seja, a gestão de riscos, por conceito, passa também a lidar com a gestão estratégica e o monitoramento contínuo dos objetivos empresariais. Os sete riscos estratégicos são:

1) Sua grande iniciativa falha
2) Seus clientes abandonam
3) Seu setor chega a uma bifurcação na estrada
4) Um concorrente aparentemente invencível aparece
5) Sua marca perde a força
6) Seu setor torna-se zona de lucro zero
7) Sua empresa para de crescer

Cada um dos riscos listados pode, simplesmente, exterminar a instituição. Isso acontece porque os riscos são menosprezados ou ignorados.

d) Risco Financeiro

Relacionado com a gestão e controle eficazes dos meios financeiros da organização e com os efeitos de fatores externos como, por exemplo, disponibilidade de crédito, taxas de câmbio, movimento das taxas de juro e outro tipo de orientações do mercado.

Conceito de Interconectividade

O relatório de Riscos Globais, do Fórum Mundial, desde 2014, salienta como os riscos globais não apenas são interconectados, mas também possuem impactos sistêmicos. Para gerir os riscos corporativos eficientemente e construir a resiliência aos seus impactos, esforços melhores são necessários para entender, medir e prever a evolução das interdependências (INTERCONECTIVIDADE) entre os riscos, suplementando as ferramentas tradicionais de gestão de riscos com novos conceitos projetados para ambientes incertos. Se os riscos não forem eficazmente abordados e interpretados, os prejuízos serão ampliados de forma geométrica e em todas as disciplinas. Podemos citar como exemplo a crise financeira de 2007/2008, onde os impactos políticos, econômicos e sociais foram de longo alcance, de forma sistêmica e de uma capilaridade avassaladora.

Para gerir os riscos corporativos eficientemente e construir a resiliência aos seus impactos, esforços melhores são necessários para entender, medir e prever a evolução das interdependências (INTERCONECTIVIDADE) entre os riscos.

A natureza sistêmica dos riscos corporativos pede por uma visão estratégica dentro da instituição. Assim como sistemas de finanças, supply-chains, saúde e energia, a internet e o ambiente se tornam mais complexos e interdependentes e seus níveis de resiliência determinam se eles se tornam o baluarte da estabilidade ou amplificadores de choques em cascata. Fortalecer a resiliência requer a superação de desafios de ação coletivos através do entendimento dos vasos comunicantes entre riscos. Podemos citar o terremoto e tsunami no Japão em 2011, onde quebrou toda a cadeia logística das empresas automobilísticas ao redor do mundo.

INDÚSTRIA AUTOMOBILÍSTICA SENTE FORTE IMPACTO DO TERREMOTO NO JAPÃO

[...] Depois do terremoto de 11 de março, nas fábricas automobilística japonesas mais de 500.000 veículos deixaram de ser fabricados, e as perdas chegaram a bilhões, segundo especialistas do setor. “A China teria perdido no final de abril 25.000 veículos; a Europa, 55.000; e a América do Norte, 68.000”, estima Carlos da Silva, analista da Global Insight, contatado pela AFP.

A maior montadora do mundo de automóveis, a japonesa Toyota, anunciou redução 50% e 70% de sua produção na China até 3 de junho de 2011.

> Os problemas na cadeia de abastecimento de componentes eletrônicos e materiais plásticos custaram à Toyota uma perda produtiva de mais de meio milhão de unidades em todo o mundo até junho de 2011. O conceito de “just in Time” ficou exposto, sendo revisado em função da interdependência.

Fonte: Disponível em: <http://g1.globo.com/mundo/noticia/2011/04/industria-automobilistica-sente-forte-impacto-do-terremoto-no-japao.html>. Acesso em: 20 out. 2017.

Desta maneira não basta mais somente utilizar a Matriz de Riscos, cruzando probabilidade e impacto, pois esta avaliação fornece a criticidade dos riscos, dentro de suas disciplinas. É importante, mas não mais só isso! Há a necessidade do entendimento da dinâmica entre riscos, ou seja da Motricidade entre eles. Quais riscos possuem força e capacidade de influenciar outros riscos. A partir daí podemos enxergar a verdadeira interconectividade entre riscos.

Sem o estudo da interconectividade, realizando o estudo somente por disciplina e ou por categoria de riscos, a empresa e seus gestores correm sérios riscos de não enxergarem os riscos sistêmicos. Risco sistêmico, segundo GOLDIN e MARIATHASAN, da Princeton University:

O risco sistêmico é o risco de ***"colapsos em um sistema inteiro, oposto ao colapso de partes e componentes individuais”.*** Os riscos sistêmicos são caracterizados por:

- Pontos de ruptura modestos, combinando indiretamente para produzir grandes falhas;
- Contágio ou compartilhamento de risco, como uma perda que desencadeia uma reação de outras;
- Sistemas sendo incapazes de recuperar o equilíbrio depois de um choque.

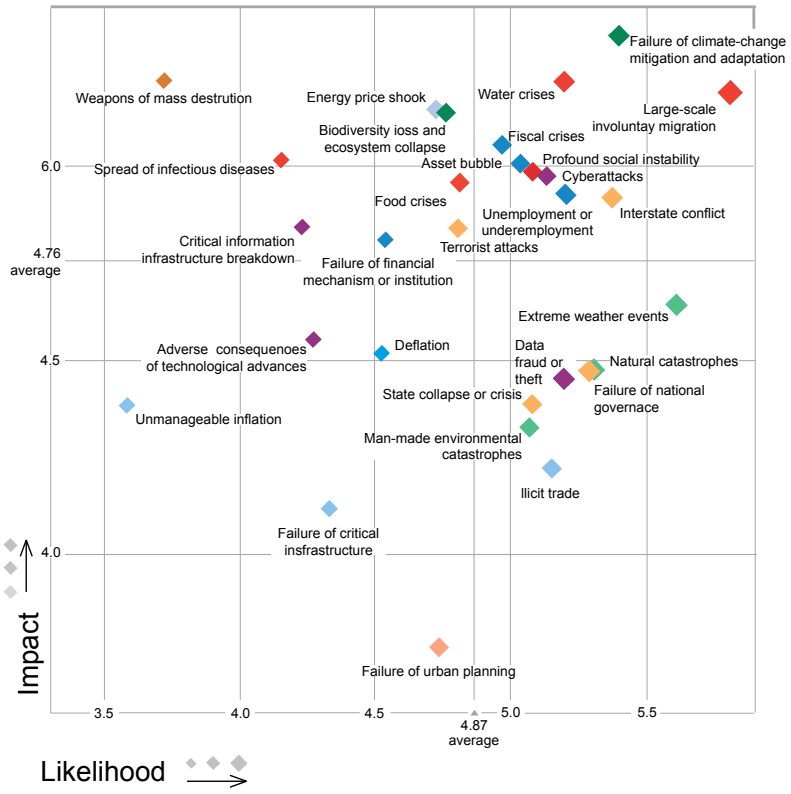
Este estudo começou na década de 1960 com o cientista Edward Lorenz, cientista do MIT - Massachusetts Institute of Technology, que na década conduzia pesquisas sobre previsão do tempo. Descobriu variações imperceptíveis nos valores da pressão e temperatura, que combinadas geravam efeitos massivos em questões de dias nas previsões do tempo. É dele a famosa pergunta: *Pode o Bater das asas de uma borboleta no Brasil causar um tornado no Texas?* O famoso Efeito Borboleta!

Portanto, o risco sistêmico está relacionado à sensibilidade de pequenas variações nas condições iniciais de um sistema, que se desenvolvem e se combinam, produzindo um enorme efeito no sistema como um todo. Ações inconsequentes, desconexas e de pouca importância nas partes de um processo podem combinar e ocasionar impactos massivos nos processos das empresas ou no modelo de negócio.

Criticidade e Motricidade de Riscos

O Relatório de Riscos Globais, mais uma vez, salienta a importância de elaborar o estudo das conexões entre riscos, ou seja, de entender as influências entre riscos. O que um risco influência em outro? Qual é a motricidade dos riscos no contexto geral do quadro? O que o Relatório sugere, que não só façamos o estudo da Matriz de Risco de probabilidade e impacto que identifica a criticidade do risco.

Figura 4 - Matriz de Riscos Globais 2016

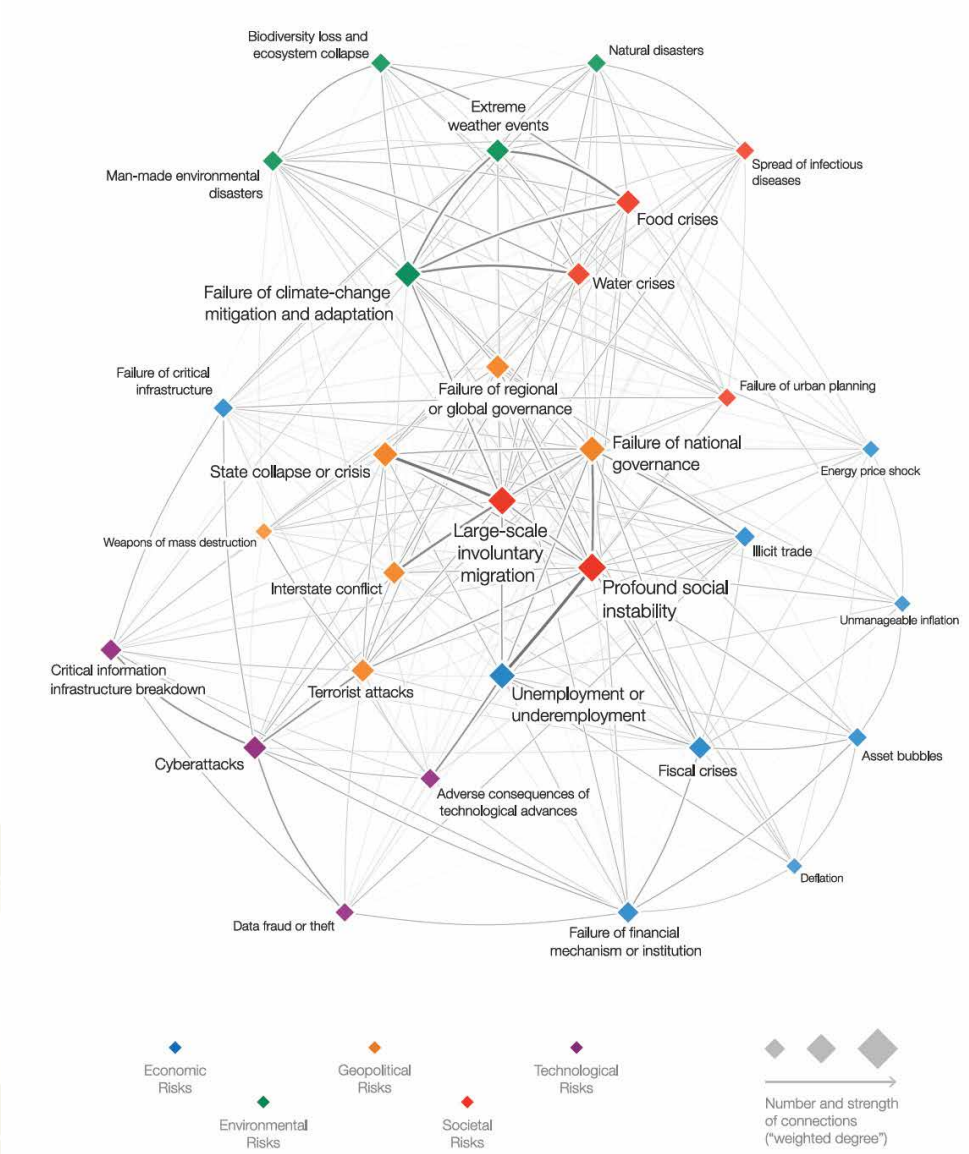


Fonte: Global Risk Report (2016).

A Matriz anterior demonstra quais riscos são mais críticos, quais são mais severos, ou seja, a Matriz de Riscos prioriza o tratamento frente a criticidade do seu impacto e probabilidade de seu acontecimento.

Podemos concluir que a influência de um risco não crítico pode, às vezes, ser estratégico, dentro de um determinado contexto. Dentro desta ótica é imperioso que o gestor passe então a enxergar a motricidade e as conexões entre os riscos. A matriz abaixo é um exemplo de motricidade entre os riscos globais.

Figura 5 - Matriz de Motricidade dos Riscos Globais 2017



Fonte: Global Risk Report (2017).

A Matriz anterior demonstra a interconectividade entre os riscos, salientando os riscos de maior motricidade, maior influência de um risco sobre o outro.

Pode-se utilizar, como metodologia em Riscos Estratégicos, o processo trazido da construção de cenários prospectivos, a Matriz de Impactos Cruzados - MIC. A MIC foi adaptada da metodologia do Cenarista francês Michael Godet que tem como base o Teorema de Bayes, Probabilidades Condicionantes.

No Processo de Gestão de Riscos - Método Brasiliano, esta ferramenta é utilizada para identificar os riscos estratégicos considerados motrizes e de ligação, ou seja, aqueles que possuem maior influência entre os demais. Ponto importante é a aplicação da ferramenta. Não se pode aplicar esta ferramenta em qualquer tipo de estudo, mas sim para estudos de riscos estratégicos e ou riscos críticos entre disciplinas. O objetivo é enxergar quais riscos são os sistêmicos.

1) A interconectividade entre riscos é resultado:

a) análise individual de cada disciplina de riscos.
b) análise da influência de um risco em outro, utilizando a ferramenta de Impactos Cruzados.
c) análise em grupo de riscos, utilizando a percepção dos gestores.
d) todas as alternativas estão corretas.

2) A Matriz de Impacto Cruzado é uma ferramenta que possui dois critérios para analisar a interconectividade dos riscos. São eles:

a) Impacto e Dependência.
b) Motricidade e Dependência.
c) Probabilidade e Impacto.
d) Motricidade e Criticidade.

3) Com a finalidade de entender a interconectividade entre os riscos é utilizada uma ferramenta que posiciona os riscos em quatro quadrantes chamada:

a) Matriz de Riscos.
b) Matriz de Priorização das Ações.
c) Matriz de Impacto Cruzado.
d) Matriz SWOT.

4) A Matriz de Priorização dos Riscos é uma ferramenta que utiliza outras duas matrizes para sua composição. Essas Matrizes fazem parte do Método Brasiliano de Análise de Riscos e são elas:

a) Matriz de Riscos e Matriz SWOT.
b) Matriz de Riscos e Matriz de Priorização das Ações.
c) Matriz de Riscos e Matriz de Impacto Cruzado.
d) Matriz de Priorização das Ações e Matriz SWOT.

Algumas Considerações

Em relação a categoria de riscos não há uma fórmula para classificar riscos, ou seja, ao existe uma classificação de riscos que seja consensual, exaustiva e aplicável a todas as organizações. A classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da indústria, mercado e setor de atuação.

Portanto, dependendo do tipo de segmento que a empresa atua podemos ter as seguintes categorias de riscos: Operacional, Legal, Estratégico e Financeiro.

Não basta somente utilizar a Matriz de Riscos, cruzando probabilidade e impacto, pois esta avaliação fornece a Criticidade dos Riscos, dentro de suas disciplinas. Também é necessário entender a dinâmica entre riscos, ou seja, da Motricidade dos Riscos entre eles, ou seja, quais riscos possuem força e capacidade de influenciar outros riscos. A partir da utilização e cruzamento das ferramentas de análise - Criticidade dos Riscos e Motricidade dos Riscos podemos enxergar a verdadeira Interconectividade entre Riscos.

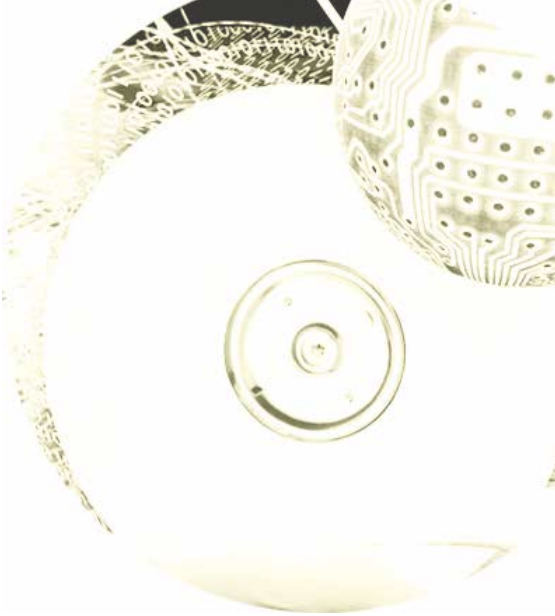
Referências

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em Riscos**: Gestão Integrada em Corporativos. São Paulo: Editora Sicurezza, 2016.

FÓRUM Econômico Mundial, Relatório de Riscos Globais, 2004.

FÓRUM Econômico Mundial, Relatório de Riscos Globais, 2017.

SLYWOTZKY, Adrian J. e WEBER, Karl. **Do risco à oportunidade**: As 7 estratégias para transformar ameaças em fatores de crescimento. Rio de Janeiro: Elservier, 2007.



Capítulo 3

Apetite ao Risco, Risco Inerente e Risco Residual

A partir da perspectiva do saber fazer, neste capítulo você terá os seguintes objetivos de aprendizagem:

- ✓ Compreender a concepção da fixação do Apetite ao Risco.
- ✓ Analisar a abrangência e aplicação do Apetite ao Risco, atrelando outras duas métricas que são a Tolerância e a Capacidade ao Risco.
- ✓ Compreender a concepção do Risco Inerente e Residual.
- ✓ Analisar a abrangência e aplicação do Risco Inerente e Residual, atrelado a necessidade de avaliação dos controles.

Contextualização

Este capítulo visa abordar a necessidade de fixação do apetite ao risco, sendo especifico para cada empresa, atrelando outras duas métricas que são a Tolerância e a Capacidade ao Risco. Destacando que a responsabilidade desta definição é do Conselho de Administração da Empresa, sugerido pela Diretoria Executiva, através do seu Presidente.

Será abordada a diferença do Risco Inerente e Residual, considerando que todas as melhores práticas nacionais e internacionais, sugerem de forma enfática que o processo de gestão de riscos deve realizar duas avaliações de riscos. Uma avaliação é a dos riscos inerentes e a outra é a dos riscos residuais.

Apetite ao Risco

Um ponto relevante da engrenagem do sistema de gerenciamento de riscos corporativos que deve estar definido e implementado em toda a instituição é a fixação do seu apetite aos riscos.

Então podemos perguntar: o que é Apetite ao Risco?

Apetite ao risco é a quantidade de risco que a empresa deseja assumir para conseguir atingir seus objetivos. Ou podemos dizer também que apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor. O apetite a risco reflete toda a filosofia administrativa de uma organização e, por sua vez, influencia a cultura e o estilo operacional desta.

Apetite ao risco é a quantidade de risco que a empresa deseja assumir para conseguir atingir seus objetivos.

A fixação do apetite ao risco permite determinar o binômio risco x benefício, controlar e manter os riscos em níveis desejados. Para tanto, para possibilitar a concretização de geração de valor nas organizações, estas devem fazer um balanço entre riscos x oportunidades x apetite ao risco, e servir de guia para a tomada de decisões, alocação de recursos e a definição do alinhamento de toda empresa para a busca dos objetivos fixados, permitindo fazer um monitoramento das ações, resultados e dos níveis de riscos associados.

Muitas organizações consideram esse apetite de forma qualitativa, categorizando-o como elevado, moderado ou baixo, enquanto outras organizações adotam uma abordagem quantitativa que reflete e equilibra as metas de crescimento, retorno e risco. Uma organização dotada de um maior apetite a risco poderá desejar alocar grande parcela de seu capital para áreas de alto risco como mercados recém-emergentes. Por outro lado, uma organização com um reduzido apetite a risco poderá limitar seu risco de curto prazo investindo apenas em mercados maduros e mais estáveis.

O apetite a risco está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de definir as estratégias, visto que estas expõem a organização a diferentes riscos.

O apetite a risco está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de definir as estratégias, visto que estas expõem a organização a diferentes riscos. O gerenciamento ajuda a administração a selecionar uma estratégia capaz de alinhar a criação de valor com o apetite a risco.

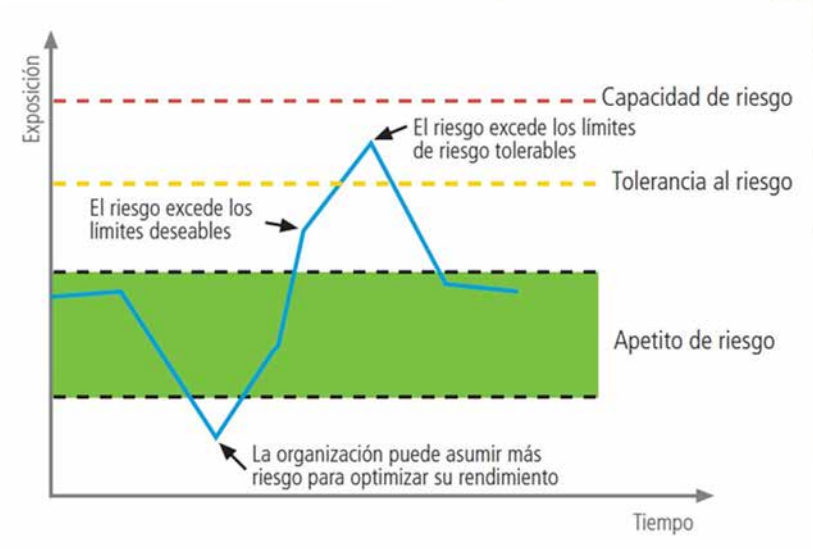
O processo de fixação do apetite ao risco é específico para cada empresa, tendo em vista que não existe um valor ou uma fórmula mágica pré-fixada que determina o respectivo apetite. A responsabilidade desta definição é do Conselho de Administração da Empresa, sugerido pela Diretoria Executiva, através do seu Presidente. Temos que levar em conta que a natureza dos riscos, do ambiente de negócios, o ambiente interno da organização, as estratégias e os objetivos de negócio, são organismos vivos que podem e devem ser revistos sempre, pois estão em constante mutação.

Tolerância e Capacidade ao Risco

O apetite é o nível de risco que a empresa quer aceitar, já a tolerância é o desvio do nível do apetite ao risco. Por outro lado, a capacidade é o nível máximo de risco que a organização pode suportar na perseguição aos seus objetivos.

Na determinação do apetite ao risco temos que possuir outras duas métricas que são a tolerância e a capacidade. Deste modo, enquanto o apetite é o nível de risco que a empresa quer aceitar, aquele com que se sente cômoda, aquele onde os gestores podem aceitar e trabalhar com tranquilidade. Já a tolerância é o desvio do nível do apetite ao risco. Por outro lado, a capacidade é o nível máximo de risco que a organização pode suportar na perseguição aos seus objetivos. Assim, a tolerância ao risco servirá como um alerta para evitar que a empresa chegue ao nível estabelecido por sua capacidade, algo que colocaria em risco a continuidade de seus negócios. O gráfico abaixo demonstra os três níveis e suas explicações.

Figura 6 - Níveis de Apetite aos Riscos



Fonte: La Fábrica de Pensamiento Instituto de Auditores Internos de España.

Outro exemplo que podemos fornecer é na própria Matriz de Riscos, com métricas qualitativas. Na Matriz de Riscos a seguir, uma empresa determinou na Política de Riscos como apetite os quadrantes laranjas (veja quadrantes com os números 1), onde os gestores precisam fazer Planos de Ações. A empresa não aceita e não Tolera Riscos (tolerância) nos quadrantes vermelhos. Porém os riscos plotados nos quadrantes com os números dois (2) são considerados no nível de Tolerância e os riscos plotados nos quadrantes com o número três (3) a Capacidade máxima.

Figura 7 - Matriz de Ricos com plotagem dos Níveis de Apetite ao Risco

Probabilidade			MUITO LEVE 1	LEVE 2	MODERADO 3	SEVERO 4	MASSIVO 5
5	ELEVADA		1	1	2	3	3
4	MUITO ALTA			1	1	2	3
3	ALTA				1	2	2
2	MÉDIA					1	2
1	BAIXA					1	1

Fonte: Brasiliano (2016, p. 88).

O que isso significa na realidade? Que os riscos nos quadrantes vermelhos não são tolerados nesta empresa. Os gestores devem fazer um esforço para que os riscos não fiquem nos quadrantes vermelhos. A diferença entre a Tolerância e a Capacidade é o nível de alerta para a criticidade, priorização e alocação de recursos, visando diminuir as possibilidades de concretização e respectivos impactos.

Atividades de Estudos:

1) O que é apetite ao risco?

_____
_____
_____
_____
_____
_____
_____
_____

2) Qual a diferença entre apetite ao risco, tolerância ao risco e capacidade ao risco?

_____
_____
_____
_____
_____
_____
_____
_____
_____

Risco Inerente

Risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. É o risco associado ao negócio e existe independente de qualquer ação tomada para sua redução.

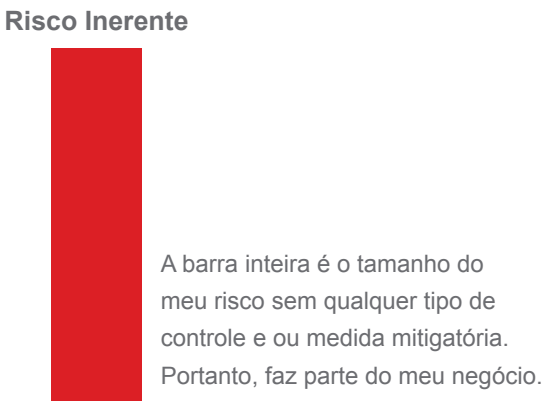
Avaliar o risco inerente significa avaliar a probabilidade e impacto da ocorrência de um risco, **desconsiderando-se a estrutura de controles atual.** Ou seja, avaliamos os riscos sem levar em consideração seus controles preventivos e ou detectivos.

Risco Residual

Risco residual é aquele que ainda permanece após a resposta da administração. É o risco remanescente após a implementação de atividades de controle que visam reduzir sua probabilidade e/ou impacto. O risco residual deve estar dentro do apetite ao risco determinado pela política da instituição.

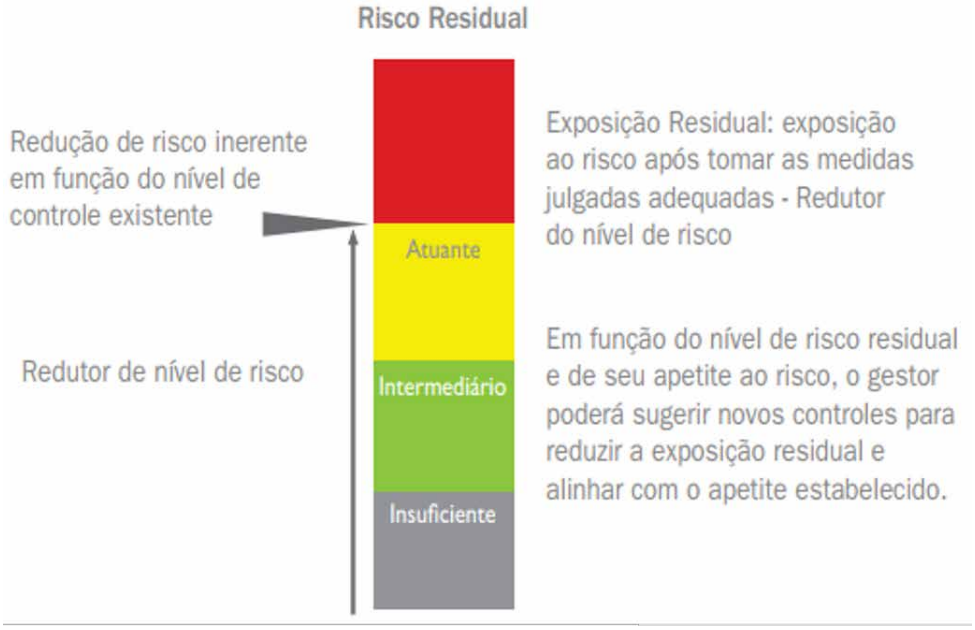
A avaliação de riscos é aplicada primeiramente aos riscos inerentes. Após a implantação de controles, reavaliaremos novamente os riscos, verificando a eficácia do respectivo controle. O gestor passará a considerar se seus riscos residuais estão dentro do apetite ao risco da empresa. Se estiver dentro do apetite ao risco, o gestor irá apenas monitorar, se estiver fora do apetite ao risco, terá que implantar, desenhar novos controles até que o residual do risco esteja dentro do respectivo apetite. No gráfico a seguir temos uma representação do risco inerente e residual.

Figura 8 - Tamanho do Risco Inerente



Fonte: Brasiliano (2016, p. 92).

Figura 9 - Risco Residual - Remanescente após as aplicações dos controles – Deve estar dentro do apetite ao risco da instituição.



Fonte: Brasiliano (2016, p. 92).

Outro conceito importante é que a diferença entre o risco inerente com o risco residual, gera o resultado da eficácia dos controles.

Atividades de Estudos:

1) O que é risco inerente?

_____
_____
_____
_____
_____
_____
_____
_____

2) O que é risco residual?

_____
_____
_____
_____
_____
_____
_____
_____

3) Caso o risco residual esteja fora do apetite ao risco, o que é necessário fazer?

_____
_____
_____
_____
_____
_____
_____
_____

Algumas Considerações

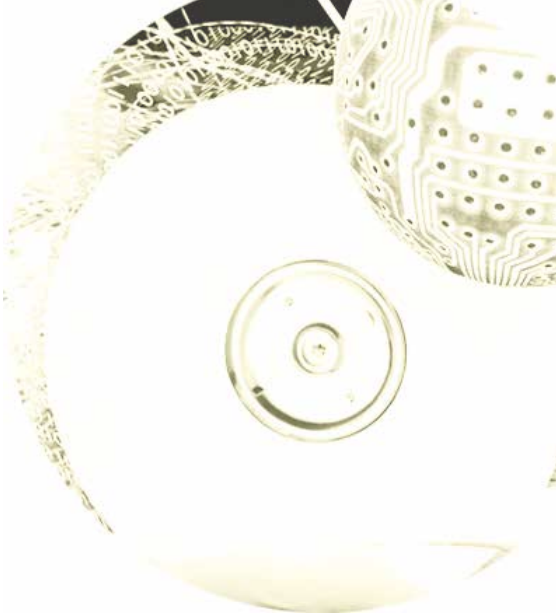
A grande importância de se ter as métricas, qualitativas e ou quantitativas de apetite, tolerância e capacidade ao risco definidas, é que com estas definições claras e objetivas, a organização está protegida de um gerente geral e ou diretor, por exemplo, ultrapassar o limite imposto.

Estas definições deverão constar na Política de Gestão de Riscos da organização, aprovada pelo Conselho e ou Presidente da Empresa, evitando quaisquer tipos de questionamento.

Necessário avaliar risco, ou seja, o tamanho do meu risco sem qualquer tipo de controle e/ou medida mitigadora, o qual é chamado de Risco Inerente e reavaliar o risco, considerando a eficácia dos controles, o qual é chamado de Risco Residual, a intenção é medir a redução do Risco Inerente e função do nível de controle existente.

Referências

BRASILIANO, Antonio Celso Ribeiro. Inteligência em Riscos: Gestão Integrada em Corporativos. São Paulo: Editora Sicurezza, 2017.



Capítulo 4

Controles Internos e Melhores Práticas - Framework's de Mercado

A partir da perspectiva do saber fazer, neste capítulo você terá os seguintes objetivos de aprendizagem:

- ✓ Compreender a concepção de Controles Internos.
- ✓ Analisar a abrangência e aplicação do Controles Internos integrado a Gestão de Riscos.
- ✓ Compreender a concepção das Melhores Práticas de Mercado.
- ✓ Analisar a abrangência e aplicação das Melhores Práticas de Mercado.

Contextualização

Este capítulo visa abordar a importância e destacando que um sistema eficaz de controle interno reduz, a um nível aceitável, o risco de não conseguir o objetivo da organização. Além disso, serão apresentadas as Melhores Práticas com os framework's.

Controle Interno

O controle interno é definido, segundo o COSO I (2013, p. 7), como sendo: "Um processo conduzido pela estrutura de governança, pela administração e por outros profissionais da entidade, e desenvolvido para proporcionar segurança razoavel com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade". Esta definição segundo COSO enfatiza conceitos fundamentais. Segundo o COSO I (2013, p. 7) o controle interno é:

- Conduzido para atingir objetivos em uma mais categorias separadas, porém sobrepostas - operacional, divulgação e conformidade.
- Um processo que consistem em tarefas e ativiades contínuas – um meio para um fim, não um fin em si mesmo.
- Realizado por pessoas - não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da organização para realizar o controle interno.
- Capaz de proporcionar segurança razoáve - mas não absoluta, para a estrutura de governança e a alta administração de uma entidade.
- Adaptável à estrutura da entidade - flexivel na aplicação, para toda a entidade ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

Esta definição é intencionalmente ampla. Ela captura os conceitos importantes que são fundamentais a como as organizações designam, implementam e conduzem os controles internos, fornecendo uma base para a aplicação, através das organizações que funcionam em diferentes estruturas, indústrias e regiões geográficas da entidade.

Integração do Controle Interno Com a Gestão de Riscos

Um sistema eficaz de controle interno reduz, a um nível aceitável, o risco de não conseguir o objetivo da organização. Ele requer que:

Os princípios relevantes do processo de gestão de riscos estejam presentes e funcionando.

- Os princípios relevantes do processo de gestão de riscos estejam presentes e funcionando. "Presente" se refere à determinação de que os componentes estejam implementados para conquistar os objetivos especificados. "Funcionando" se refere à determinação de que os princípios relevantes continuem a existir nas operações e nos processos.

Os princípios do processo de gestão de riscos funcionam juntos e de uma forma integrada.

- Os princípios do processo de gestão de riscos funcionam juntos e de uma forma integrada. "Funcionar juntos" se refere à determinação de que todos os princípios reduzam, a um nível aceitável, o risco de não conquistar os objetivos. Os componentes do processo de gestão de riscos são interconectados e ligações entre eles, particularmente na forma pela qual os princípios interagem dentro e através deles.

Quando um sistema de controle interno é determinado como sendo eficaz, a gestão sênior e o conselho de diretores possuem uma garantia razoável, relativa à aplicação dentro da estrutura da entidade, de que a organização:

- Conquista operações eficazes e eficientes quando os eventos externos são considerados improváveis de possuírem impacto significante sobre a conquista dos objetivos ou onde a organização possa predizer razoavelmente a natureza e a duração dos eventos externos e mitigar o impacto a um nível aceitável.

- Compreender a extensão a qual as operações são administradas eficazmente e eficientemente quando os eventos externos possam possuir um impacto significante sobre a conquista dos objetivos ou onde a organização possa predizer razoavelmente a natureza e a duração dos eventos externos e mitigar o impacto a um nível aceitável.

- Prepara relatórios em conformidade com as regras, regulamentos e normas aplicáveis ou com os objetivos de relatório especificados da entidade.

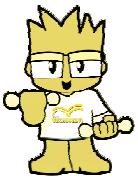
- Concorda com as leis, regras, regulamentos e normas externas aplicáveis.

O processo de gestão de riscos deve realizar, de forma contínua, o julgamento na projeção, implementação e condução do controle interno e na avaliação de sua eficácia. O uso do julgamento, dentro das fronteiras estabelecidas pelas leis, regras, regulamentos e normas, melhora a habilidade da gestão de tomar decisões melhores acerca do controle interno, mas sem garantir resultados perfeitos.

O processo de gestão de riscos da organização tem que reconhecer, fazendo parte da boa prática de mercado, que embora o controle interno forneça garantia razoável de conquistar os objetivos, as limitações existem. O controle interno não pode prevenir o mal julgamento ou as más decisões, ou os eventos externos que podem fazer uma organização falhar em conquistar os seus objetivos operacionais. Em outras palavras, mesmo um sistema eficaz de controle interno pode experimentar uma falha. As limitações podem resultar de:

- Adequação de objetivos estabelecidos como uma precondição ao controle interno.
- Da realidade de que o julgamento humano na tomada de decisão pode ser defeituoso e sujeito a preconceito.
- Rupturas que possam acontecer por falhas humanas, como erros simples.
- Da habilidade da gestão em substituir o controle interno.
- Da habilidade da gestão, outro pessoal, e/ou terceiros em lograr os controles através do conluio.
- Eventos externos além do controle da organização.

Essas limitações impedem o conselho e a gestão de possuir uma garantia absoluta da conquista dos objetivos da entidade - isto é, o controle interno fornece **garantia razoável, mas não absoluta.** Não bastasse essas limitações inerentes, a gestão deve estar ciente delas quando selecionar, desenvolver e empregar controles que minimizem, à extensão prática, essas limitações.



Atividades de Estudos:

1) O que é Controle Interno, segundo o COSO?

_____
_____
_____
_____
_____
_____
_____
_____

Coso - Committee of Sponsoring Organizations of the Treadway Commission

O COSO é uma organização privada criada nos Estados Unidos em 1985 para previnir e evitar fraudes nas demonstrações contábeis da empresa.

O COSO é uma organização privada criada nos Estados Unidos em 1985 para previnir e evitar fraudes nas demonstrações contábeis da empresa. Portanto é uma antiga organização brigando para o quesito prevenção a fraudes, e as empresas, na realidade, fazem muito pouco para o processo preventivo acontecer.

O foco do COSO é a implantação de controles internos efetivos, proporcionando uma garantia razoável para previnir fraudes.

O foco do COSO é a implantação de controles internos efetivos, proporcionando uma garantia razoável para previnir fraudes. Em 1985, foi criada nos Estados Unidos a National Commission on Fraudulent Financial Reporting – Comissão Nacional sobre Fraudes em Relatórios Financeiros – iniciativa independente para estudar as causas da corrência de fraudes em relatórios financeiros e contábeis. Essa comissão era composta de representantes das principais associações de classe de profissionais ligados à área financeira. Seu primeiro objeto de estudo foram os controles internos.

O COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros fundamentados na ética, na efetividade dos controles internos e na governança corporativa, além de ser patrocinado por cinco das principais associações de classe:

- AICPA - American Institute of Certified Public Accounts – Instituto Americano de Contadores Públicos Certificados;
- AAA - American Accounts Association - Associação Americana de Contadores;
- FEI - Financial Executive International - Executivos Financeiros Internacionais;
- IIA - The Institute of Internal Auditors – Instituto dos Auditores Inernos;
- IMA - Institute of Management Accountants – Instituto de Contadores Gerenciais.

O comitê trabalha com independência em relação a suas atividades patrocinadoras.

Coso I - Conceito e a Revisão 2013

É reconhecido como um framework pioneiro pelo designing, pela implementação e pela condução do controle interno e a avaliação da eficácia do controle interno.

Em 1992, o Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO) lançou o seu *Controle Interno - Framework Integrado*. O *framework* original ganhou uma ampla aceitação e é amplamente utilizado ao redor do mundo. É reconhecido como um *framework* pioneiro pelo *designing*, pela implementação e pela condução do controle interno e a avaliação da eficácia do controle interno.

Nos vinte anos desde a sua criação, o *framework* original, os negócios e os ambientes operacionais mudaram dramaticamente, se tornando cada vez mais complexos, movidos tecnológica e globalmente.

Ao mesmo tempo, as partes interessadas estão mais envolvidas, buscando uma transparência e contabilidade maiores para a integridade dos sistemas do controle interno que suportam as decisões e a governança da organização.

O COSO acredita que o *Framework* de Controles Internos permitirá que as organizações desenvolvam e mantenham eficazmente os sistemas de controle interno que podem melhorar a probabilidade de conquistar os objetivos da entidade e adaptar-se às mudanças nos negócios e nos ambientes operacionais. Ele retém a definição primária do controle interno e os seus cinco componentes. O requerimento para considerar os cinco componentes para avaliar a eficácia de um sistema de controle interno permanecem imutáveis, fundamentalmente.

O *Framework* continua a enfatizar a importância do julgamento da gestão no *designing*, implementação e condução do controle interno, e na avaliação da eficácia de um sistema de controle interno.

Ao mesmo tempo, o *Framework* inclui melhorias e esclarecimentos que tencionam facilitar o uso e a aplicação. No *Framework* atualizado, esses conceitos são agora princípios, os quais são associados com os cinco componentes, e os quais fornecem esclarecimento para o usuário na projeção e na implementação dos sistemas de controle interno e para compreender os requerimentos para o controle interno eficaz.

O *Framework* foi melhorado ao expandir a categoria de relatório financeiro de objetivos, para incluir outras formas importantes de relatório, como o não-financeiro e o relatório interno. Além disso, o *Framework* reflete as considerações de muitas mudanças nos negócios e nos ambientes operacionais nas várias décadas passadas, incluindo:

- Expectativas para a fiscalização da Governança
- Globalização dos mercados e das operações
- Mudanças e maiores complexidades dos negócios
- Demandas e complexidades nas leis, regras, regulamentos e normas
- Expectativas para competências e contabilidades
- Uso de, e dependência de, tecnologias em evolução
- Expectativas relacionadas à prevenção e detecção da fraude

a) Conceito da Estrutura de Controle Interno - *Framework* do COSO I

O controle interno auxilia as entidades a conquistarem os objetivos importantes e a sustentarem e melhorarem o desempenho.

O controle interno auxilia as entidades a conquistarem os objetivos importantes e a sustentarem e melhorarem o desempenho. O *Controle Interno - Framework Integrado* do COSO I permite que as organizações desenvolvam eficaz e eficientemente sistemas de controle interno que se adaptem ao negócios e ambientes operacionais mutáveis, mitiguem riscos a níveis aceitáveis e apóiem tomadas de decisões razoáveis e a governança da organização.

Projetar e implementar um sistema eficaz de controle interno pode ser um grande desafio; usar esse sistema eficaz e eficientemente todos os dias pode ser intimidador. Novos modelos de negócios rapidamente mutáveis, um uso maior e a dependência da tecnologia, requerimentos regulatórios e escrutínio elevados, globalização e outros desafios exigem que um sitema de controle interno seja ágil na adaptação às mudanças nos negócios e nos ambientes regulatórios e operacionais.

Um sistema eficaz de controle interno exige mais do que uma aderência rigorosa às políticas e aos procedimentos: exige o uso do julgamento.

Um sistema eficaz de controle interno exige mais do que uma aderência rigorosa às políticas e aos procedimentos: exige o uso do julgamento. A gestão e a diretoria usam o julgamento para determinar o

quanto de controle é o suficiente. A gestão e outro pessoal usam o julgamento todos os dias para selecionar, desenvolver e empregar controles através da entidade. A gestão e os auditores internos, entre outro pessoal, aplicam o julgamento enquanto monitoram e avaliam a eficácia do sistema do controle interno.

O *Framework* auxilia a gestão, os conselhos, a diretoria, as partes interessadas externas e outros a interagir com a entidade em seus respectivos deveres com relação ao controle interno, sem ser demasiado prescritivo. Para a gestão, os conselhos e diretoria, o *Framework* fornece:

- Formas de aplicar o controle interno a qualquer tipo de entidade, independente da indústria ou da estrutura legal, aos níveis da entidade, unidade operacional ou função;

- Uma abordagem baseada em princípios que forneça flexibilidade e permite o julgamento na projeção, implementação e condução dos princípios do controle interno que possam ser aplicados à entidade, a níveis operacionais e funcionais;

- Requerimentos para um sistema eficaz de controle interno ao considerar como os componentes e princípios estão presentes e funcionando, e como os componentes funcionam juntos;

- Formas de identificar e analisar os riscos, e de desenvolver e administrar respostas adequadas aos riscos dentro de níveis aceitáveis e com foco maior em medidas anti-fraude (diga-se que é a primeira estrutura a enfatizar a necessidade de gerir o risco de fraude nas organizações);

- Uma oportunidade para expandir a aplicação do controle interno além do relatório financeiro para outras formas de relatório, operações e objetivos de concordância;

- Uma oportunidade para eliminar controles ineficazes, redundantes ou ineficientes que forneçam valor mínimo à redução de riscos à conquista dos objetivos da entidade.

Para as partes interessadas externas de uma entidade e outros que interajam com a entidade, a aplicação do *Framework* fornece:

- Maior confiança no discernimento da diretoria dos sistemas de controle interno;
- Maior confiança com relação à conquista dos objetivos;

- Maior confiança na habilidade da organização em identificar, analisar e responder ao risco e às mudanças nos ambientes comerciais e operacionais;
- Maior compreensão do requerimento de um sistema eficaz de controle interno;
- Maior compreensão de que, através do uso do julgamento, a gestão possa ser capaz de eliminar controles ineficazes, redundantes ou ineficientes.

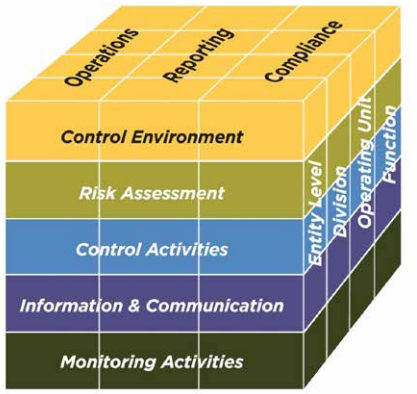
O controle interno não é um processo em série, mas um processo dinâmico e integrado. O *Framework* se aplica a todas as entidades: órgãos grandes, medianos, pequenos, lucrativos, não lucrativos e governamentais. Entretanto, cada organização pode escolher implementar o controle interno diferentemente. Por exemplo, um sistema menor da entidade do controle interno pode ser menos formal e menos estruturado e ainda assim possuir um controle interno eficaz.

b) O Framework do COSO I

O Framework do COSO I possui como elementos:

1) Objetivos
2) Elementos do Processo
3) Áreas da empresa que são atingidas pela disseminação dos princípios.

Figura 10 - *Framework* do COSO I



Fonte: Brasiliano (2016 apud Framework COSO I, 1982, p. 59).

Objetivos: O *Framework* fornece três categorias de objetivos, as quais permitem que as organizações se foquem em diferentes aspectos de controle interno:

- Objetivos das Operações - Esses pertencem à eficácia e à eficiência das operações da entidade, incluindo os objetivos de desempenho operacional e da garantia dos ativos contra o prejuízo;

- Relatando Objetivos - Esses pertencem aos relatórios financeiros internos e externos e não financeiros, e podem abranger a confiança, a durabilidade, a transparência ou outros termos como estabelecidos pelos reguladores, organismos de normalização reconhecidos ou políticas da entidade;

- Objetivos de *compliance* - Esses pertencem à aderência às leis e regulamentos aos quais a entidade é sujeita.

c) Componentes do Controle Interno

O controle interno consiste de cinco componentes integrados.

- **Ambiente de Controle:** O ambiente de controle é o conjunto de normas, processos e estruturas que fornecem a base para desempenhar o controle através da organização. O conselho de diretores e a gestão sênior estabelecem o tema com relação à importância do controle interno, incluindo as normas esperadas de conduta. A gestão reforça as espectativas nos vários níveis da organização. O ambiente de controle compreende a integridade e os valores éticos da organização; os parâmetros que permitem que o conselho de diretores empreendam as suas responsabilidades de fiscalização de governança; a estrutura organizacional e o emprego de autoridade e responsabilidade; o processo para atrair, desenvolver e reter os indivíduos competentes; e o rigor acerca das medidas de desempenho, incentivo e recompensas para mover a contabilidade pelo desempenho. O ambiente de controle resultante possui um impacto persistente sobre o sistema total de controle interno.

- **Avaliação de Riscos:** Cada entidade confronta uma variedade de riscos de fontes internas e externas. A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e avaliar os riscos para conquistar os objetivos. O riscos para a conquista desses objetivos através da entidade são considerados relativos às tolerâncias de riscos estabelecidos. Portanto, a avaliação de riscos forma a base para determinar como os riscos serão gerenciados. Uma pré-condição à avaliação de riscos é o estabelecimento de objetivos, ligados a diferentes

níveis da entidade. A gestão especifica os objetivos dentro de categorias que se relacionam às operações, relatórios e conformidade com clareza o suficiente para ser capaz de identificar e analisar os riscos desses objetivos. A gestão também considera a adequação dos objetivos para a entidade. A avaliação de riscos também exige que a gestão considere o impacto de possíveis mudanças no ambiente externo e dentro de seu próprio modelo comercial que possa tornar o controle interno ineficaz.

- **Atividades de Controle:** As atividades de controle são as ações estabelecidas através das políticas e dos procedimentos que ajudam a assegurar as diretrizes da gestão para diminuir a probabiidade e mitigar os riscos para que a conquista dos objetivos seja desempenhada. As atividades de controle são desempenhadas em todos os níveis da entidade, em vários estágios dentro dos processos comerciais e através do ambiente tecnológico. Elas podem ser preventivas ou detectivas em natureza e podem abranger uma gama de atividades manuais ou automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho comerciais. A segregação de tarefas é normalmente construída na seleção e no desenvolvimento das atividades de controle. Onde a segregação de tarefas não for prática, a gestão seleciona e desenvolve atividades de controle alternativas.

- **Informação e Comunicação:** A informação é necessária para que a entidade desempenhe as responsabilidades de controle interno para apoiar a conquista de seus objetivos. A gestão obtém ou gera e usa a informação relevante e de qualidade de ambas as fontes internas e externas para apoiar o funcionamento de outros componentes do controle interno. A comunicação é um processo contínuo e interativo de fornecimento, compartilhamento e obtenção de informação necessária. A comunicação interna é a forma pela qual a informação é disseminada através da organização, fluindo através da entidade. Ela permite que o pessoal receba uma mensagem clara da gestão sênior que controla as responsabilidade e que devem ser levadas a sério. A comunicação externa é dupla: permite a comunicação de entrada de informação externa relevante e fornece informação à partes externas em resposta a requerimentos e expectativas.

- **Monitoramento de Atividades:** As avaliações em andamento, separadas ou alguma combinação das duas, são utilizadas para garantir se cada um dos cinco componentes do controle interno, incluindo os controles para efetivar os princípios dentro de cada componente, estão presentes e funcionando. As avaliações em andamento, construídas nos processos comerciais a diferentes níveis da entidade, fornecem uma informação em tempo hábil.

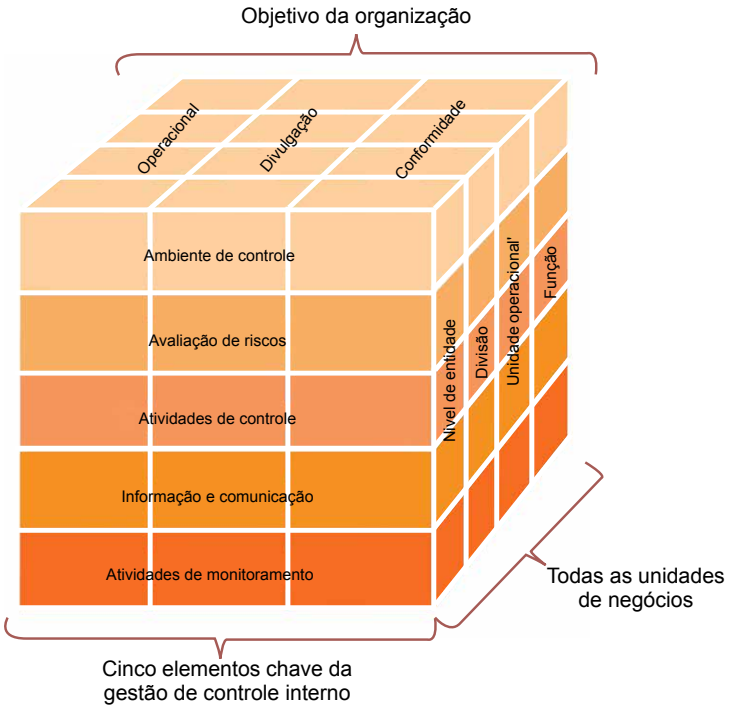
Avaliações separadas, conduzidas periodicamente, variarão em escopo e frequência, dependendo da avaliação dos riscos, eficácia de avaliações em andamento e outras considerações da gestão. As descobertas são avaliadas contra os critérios estabelecidos pelos reguladores, órgãos legisladores reconhecidos ou a gestão e o conselho de diretores, e as deficiências são comunicadas à gestão e ao conselho de diretores conforme o adequado.

d) Relação de Objetivos e Componentes

Uma relação direta existe entre os *objetivos*, os quais são o que uma entidade luta para conseguir, os, *componentes*, os quais representam o que é exigido para conquistar os objetivos e a *estrutura organizacional* da entidade (as unidades operacionais, as entidades legais e outros).

- As três categorias de objetivos - operações relatórios e *compliance* - são representados pelas colunas.
- Os cinco componentes são representados pelas fileiras (linhas).
- A estrutura organizacional de uma entidade é representada pela terceira dimensão.

Figura 11 - Framework do COSO I - 2013



Fonte: Brasiliano (2016 apud Framework COSO I, 2013, p. 63).

e) Componentes e Princípios

O Framework COSO I estabelece 17 (dezessete) princípios representando os conceitos fundamentais associados a cada componente. Por esses princípios serem extraídos diretamente dos componentes, uma empresa pode conseguir um controle interno eficaz ao aplicar todos os princípios. Todos os princípios se aplicam às operações, relatórios e objetivos de conformidade. Os princípios apoiando os componentes do controle interno são listados a seguir.

- **Ambiente de Controle**

1) A organização demonstra um compromisso com a integridade e valores éticos.
2) O conselho de diretores demonstra independência da gestão e exercita a fiscalização do desenvolvimento e desempenho do controle interno.
3) A gestão estabelece, com a fiscalização do conselho, estruturas, linhas de relatório e autoridades e responsabilidades adequadas na conquista dos objetivos.
4) A organização demonstra um comprometimento para atrair, desenvolver e reter indivíduos competentes juntos com os objetivos.
5) A organização mantém os indivíduos responsáveis pelas suas responsabilidades de controle interno na conquista dos objetivos.

- **Avaliação de Riscos**

6) A organização especifica objetivos com clareza o suficiente para permitir a identificação e a avaliação dos riscos relacionados aos objetivos.
7) A organização identifica os riscos para a conquista dos seus objetivos através da entidade e analisa os riscos como uma base para determinar como os riscos devem ser administrados.
8) A organização considera o potencial para a fraude na avaliação dos riscos para conseguir os objetivos (O Princípio 8 ressalta a importância da empresa gerenciar o risco de fraude, sendo a única estrutura de controle que descreve especificamente a questão do risco de fraude. Portanto os gestores de riscos e auditores devem abrir uma disciplina específica de Risco de Fraude).
9) A organização identifica e avalia as mudanças que poderiam impactar significantemente no sistema de controle interno.

- **Atividades de Controle**

10) A organização seleciona e desenvolve atividades de controle que contribuem à mitigação de riscos para a conquista dos objetivos a níveis aceitáveis.
11) A organização seleciona e dessenvolve atividades gerais de controle sobre a tecnologia para apoiar a conquista de objetivos.
12) A organização emprega atividades de controle através de políticas que estabeleçam o que é esperado e procedimentos que coloquem as políticas em ação.

- **Informação e Comunicação**

13) A organização obtém ou gera e usa informação relevante e de qualidade para sustentar o funcionamento do controle interno.
14) A organização comunica internamente a informação, incluindo objetivos e responsabilidades pelo controle interno, necessários para apoiar o funcionamento do controle interno.
15) A organização se comunica com as partes externas com relação às questões afetando o funcionamento do controle interno.

- **Atividades de Monitoramento**

16) A organização seleciona, desenvolve e desempenha avaliações em andamento/e ou separadas para se certificarem de que os componentes do controle interno estão presentes e funcionando.
17) A organização avalia e comunica as deficiências do controle interno em tempo hábil às partes responsáveis por tomarem medidas corretivas, incluindo a gestão sênior e o conselho de diretores, conforme o adequado.

A utilização do *Framework* de forma integrada, proporciona para a empresa uma estrutura de controle interno eficaz, mitigando de forma direta, tanto riscos oriundos de erros e displicência como com a intenção de praticar desvios de conduta – a fraude.

Coso II ERM - Enterprise Risk Management

O COSO lançou em 2004 uma estrutura mais ampla, com um espectro mais estratégico. Esta estrutura foi concebida para suportar o gerenciamento de riscos com uma visão corporativa, abrangendo todo e qualquer categoria de riscos.

a) Componentes do Gerenciamento de Riscos - Metodologia COSO - ERM

O gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados, segundo a Metodologia COSO – ERM (Enterprise Risk Management), são eles:

- **Ambiente Interno:** O ambiente interno compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente em que estes estão.

- **Fixação de Objetivos:** Os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos.

- **Identificação de Eventos:** Os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos.

- **Avaliação de Riscos:** Os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais.

- **Resposta a Risco:** A administração escolhe as respostas aos riscos - evitando, aceitando, reduzindo ou compartilhando – desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco.

- **Atividades de Controle:** Políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia.

- **Informações e Comunicações:** As informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos níveis da organização.

- **Monitoramento:** A integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas.

A rigor, o gerenciamento de riscos corporativos não é um processo em série pelo qual um componente afeta apenas o próximo. É um processo multidirecional e interativo, segundo o qual quase todos os componentes influenciam os outros.

b) Relacionamento entre Objetivos e os Componentes da Metodologia COSO - ERM

Existe um relacionamento direto entre os objetivos que uma organização empenha-se em alcançar, e os componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance. Esse relacionamento é apresentado em uma matriz tridimensional em forma de cubo.

As quatro categorias de objetivos (estratégicos, operacionais, de comunicação e conformidade) estão representadas nas colunas verticais. Os oito componentes nas linhas horizontais e as unidades de uma organização na terceira dimensão. Essa representação ilustra a capacidade de manter o enfoque na totalidade do gerenciamento de riscos de uma organização, ou na categoria de objetivos, componentes, unidade da organização ou qualquer um dos subconjuntos.

Figura 12 - Framework do COSO II - 2004

Fonte: Brasiliano (2016 apud Framework COSO II, 2013, p. 67).

ISO 31000

Durante os anos de 2007 e 2008 uma série de questões de riscos - desde a crise de liquidez nos mercados financeiros até as preocupações emergentes sobre terrorismo, clima, disponibilidade de alimentos, infraestrutura e energia, focou a atenção global na fragilidade da sistêmica dos processos estratégicos das nações e consequentemente do mundo.

Uma conscientização do risco e gerenciamento de risco é cada vez mais vista como um pré-requisito para controle efetivo tanto no setor privado como no público.

Dentro deste contexto é que a ISO 31000 foi concebida, possuindo como desafio integrar os diferentes conceitos da Gestão de Riscos. A norma foi desenvolvida por uma comissão especial da ISO *(International Organization for Standardization)* e teve sua numeração definida como ISO 31000.

A ISO 31000 pode ser aplicada por empresas de qualquer tipo, tamanho ou área de atuação, lidando com as incertezas que podem afetar os seus objetivos.

A ISO 31000 surgiu da necessidade de harmonizar padrões, regulamentações e *frameworks* publicados anteriormente e que de alguma forma estão relacionados com a gestão de riscos. A ISO 31000 pode ser aplicada por empresas de qualquer tipo, tamanho ou área de atuação, lidando com as incertezas que podem afetar os seus objetivos.

Estes objetivos podem estar relacionados com várias atividades da organização, desde as iniciativas estratégicas como as atividades operacionais, processos ou projetos. Assim, a norma pode ser aplicada aos vários tipos de riscos ligados aos diferentes setores da organização, tais como: financeiro, saúde e meio ambiente, tecnologia da informação, segurança empresarial, seguros, e de projetos, entre outros, incluindo a visão moderna de que risco também é oportunidade.

A ISO 3100 surge também para integrar as diversas metodologias e terminologias, pois hoje ainda há falta de consenso em relação à terminologia e aos conceitos utilizados para a gestão de riscos.

O resultado mais comum dessa equação é que a gestão de riscos acaba sendo tratada de forma isolada, fazendo com que vários gestores (saúde, meio ambiente, segurança de TI e empresarial, legal, financeiro, seguros, entre outros) trabalhem em ilhas departamentais, o que ocasiona a utilização de terminologias, sistemas, critérios e conceitos diferentes para cada uma das áreas da empresa. Ou seja, cada departamento não possui o denominado impacto cruzado, não enxerga o impacto do risco que está estudando em outras áreas e/ou processos.

A ISO 31000 possui um processo consistente e uma estrutura abrangente para ajudar a assegurar que o risco será gerenciado de forma eficaz, eficiente e coerentemente. Por esta razão a abordagem é genérica, fornecendo os princípios e diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto. A ISO 31000 descreve as possibilidades da gestão de riscos nas empresas:

A ISO 31000 possui um processo consistente e uma estrutura abrangente para ajudar a assegurar que o risco será gerenciado de forma eficaz, eficiente e coerentemente.

- aumentar a probabilidade de atingir os objetivos;
- encorajar uma gestão proativa;
- estar atento para a necessidade de identificar e tratar os riscos através de toda organização;
- melhorar a identificação de oportunidades e ameaças;
- atender às normas internacionais e requisitos e regulamentos pertinentes;
- melhorar o reporte das informações financeiras;
- melhorar a governança;
- melhorar a confiança das partes interessadas;
- estabelecer uma base confiável para a tomada de decisão e o planejamento;
- melhorar os controles;
- alocar e utilizar eficazmente os recursos para o tratamento dos riscos;
- melhorar a eficácia e a eficiência operacional;
- melhorar o desempenho em saúde e segurança, bem como proteção ao meio ambiente;

- melhorar a prevenção de perdas e a gestão de incidentes;
- minimizar perdas;
- melhorar a aprendizagem organizacional; e
- aumentar a resiliência da organização.

a) Organização da Norma

A norma possui a seguinte organização:

Introdução

1) Escopo
2) Termos e Definições
3) Princípios
4) Estrutura
5) Processo
6) Anexos: A Atributos de uma gestão de riscos avançada

b) Estrutura

O sucesso da gestão de riscos depende da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda organização, em todos os níveis. A estrutura descreve os componentes necessários para gerenciar riscos e a forma como eles se inter-relacionam. O diagrama abaixo foi retirado da ISO 31000, onde explica a estrutura necessária para fazer o processo de gestão de riscos corporativos nas empresas.

Figura 13 - Componentes da ISO 31000

Relacionamento entre os componentes da estrutura para gerenciar riscos

Fonte: Brasiliano (2016 apud ISO 31000, 2009, p. 72).

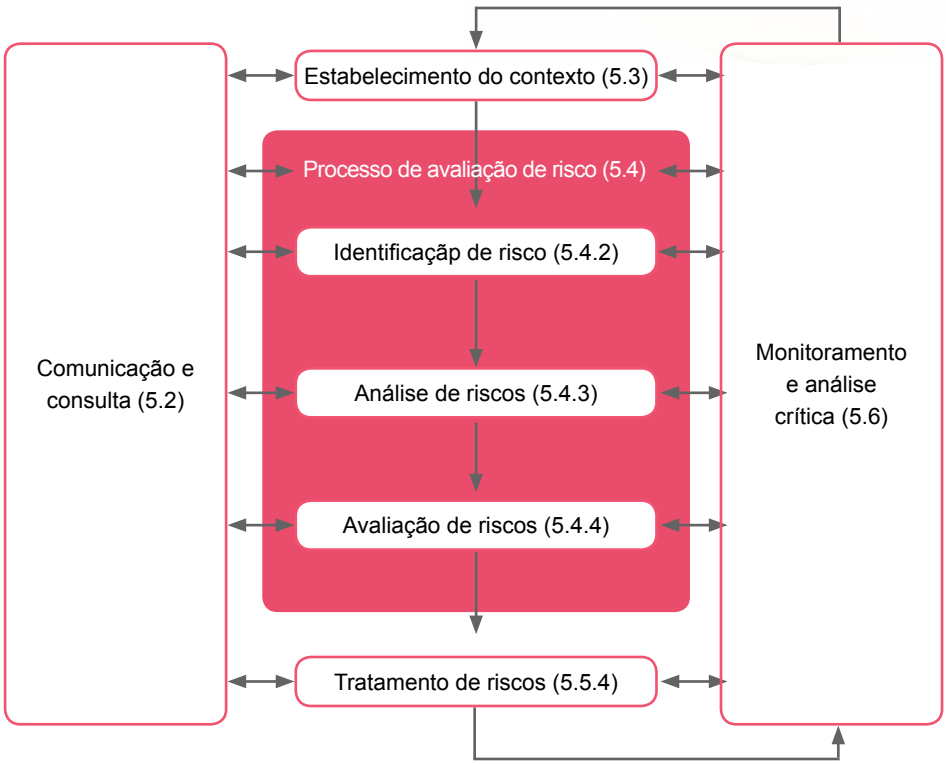
c) Processo

O processo de Gestão de Riscos da ISO 31000 foi elaborado para ser:

- parte integrante da gestão;
- incorporado na cultura e nas práticas, e
- adaptado aos processos de negócio da organização.

Ele compreende as atividades apresentadas na figura a seguir:

Figura 14 - Framework da ISO 31000



Processo de Gestão de Riscos

Fonte: Brasiliano (2016 apud ISO 31000, 2009, p. 73).

Genericamente o processo estruturado sugerido possui sete fases claramente identificadas, sendo um processo retroalimentativo. Ou seja, segue os princípios do ciclo da qualidade, PDCA: Plan - Do - Check - Action.

A fase de comunicação e consulta abrange todas elas e é inter-relacionada.

A fase de comunicação e consulta abrange todas elas e é inter-relacionada. Abrange tanto a comunicação interna e externa, assegurando que os responsáveis e partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as respectivas razões.

A fase do estabelecimento do contexto é entender os fatores e as variáveis externas

A fase do estabelecimento do contexto é entender os fatores e as variáveis externas, incluindo os fatores chaves, as tendências e as relações com as partes interessadas externas e suas percepções de valores. Já no contexto interno é entender seus objetivos estratégicos, a cultura, processos, estrutura e estratégia. No contexto estratégico estabelece o processo de gestão de riscos com sua estrutura, seus critérios e métodos que a organização deverá utilizar. Definem-se metas e objetivos além de responsabilidades e o apetite ao risco que a organização quer possuir.

A fase da identificação de riscos, no processo de avaliação de riscos, é a listagem dos riscos, com as respectivas fontes de riscos.

A fase da identificação de riscos, no processo de avaliação de riscos, é a listagem dos riscos que o processo, departamento e ou empresa possui com as respectivas fontes de riscos. A identificação deve ser crítica, pois um risco que não é identificado nesta fase não será incluído em análises posteriores. Fica claro que esta é a fase estratégica pois é nesta que se entende os fatores de riscos, os fatores facilitadores da existência do risco na empresa.

A fase de análise de riscos desenvolve a compreensão dos riscos.

A fase de análise de riscos desenvolve a compreensão dos riscos. Com a compreensão dos riscos é que a empresa poderá tomar decisão sobre seu tratamento. Nesta fase, estima-se a Probabilidade e Consequência do risco na empresa. A análise envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. A norma não especifica critérios e métodos, sendo que a organização é que deve escolher, tendo em vista as características do negócio.

A fase da avaliação de riscos é para auxiliar na tomada de decisões com base nos resultados da análise de riscos

A fase da avaliação de riscos é para auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. A avaliação de riscos envolve comparar o nível de risco encontrado durante a análise de riscos. Deve-se utilizar uma Matriz de Riscos como ferramenta de gestão. A fase de Tratamento de Riscos envolve um processo cíclico composto por:

- a avaliação do tratamento já realizado;
- a decisão se os níveis de risco residual são toleráveis;

- se não forem toleráveis, a definição e implementação de um novo tratamento;
- a avaliação e eficácia desse tratamento.

As opções de tratamento são as universais:

- a ação de evitar o risco;
- a tomada ou aumento do risco – se o risco for positivo;
- a remoção da fonte de riscos;
- a alteração da probabilidade;
- a alteração das consequências;
- o compartilhamento do risco; e
- a retenção do risco por uma decisão consistente e bem embasada.

A última fase, monitoramento e análise crítica, é a fase da checagem ou das vigilâncias regulares. Podem ser regulares – periódicas ou acontecerem em resposta a um fato específico. Deve haver uma definição clara e direta das responsabilidades de quem vai realizar o monitoramento e análise crítica.

d) Registros do Processo de Gestão de Riscos

As atividades de gestão de riscos devem ser rastreáveis. Ou seja, deve haver registros, pois estes fornecem os fundamentos para melhoria dos métodos e ferramentas, bem como de todo o processo.

Atividades de Estudos:

1) As três estruturas de controle e gestão de riscos, hoje utilizadas como benchmarking de mercado são:

a) ISO 31000, ISO 31010 e COSO IV.
b) COSO I, COSO II e ISO 31000.
c) ISO 31000, ISO 14000, ISO 26000.
d) ISO 31000, COSO II, COBIT.

2) Quais das estruturas abaixo descreve especificamente que a empresa deve avaliar riscos de fraude?

a) ISO 31000.
b) COSO II.
c) COSO I.
d) todas as alternativas estão corretas.

3) Quais são as etapas do framework da norma ISO 31000?

a) Estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos e monitoramento e análise crítica.
b) Comunicação e consulta, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, monitoramento e análise crítica e estabelecimento do contexto.
c) Comunicação e consulta, estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos e monitoramento e análise crítica.
d) Comunicação e consulta, análise situacional, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos e monitoramento e análise crítica.

Algumas Considerações

O controle interno é um processo efetivado pelo conselho de diretores de uma entidade, pela gestão e outro pessoal, designado a fornecer garantia razoável com relação à conquista de objetivos relacionados à operações, relatório e concordância.

Um sistema eficaz de controle interno reduz, a um nível aceitável, o risco de não conseguir o objetivo da organização.

O processo de gestão de riscos deve realizar, de forma contínua, o julgamento na projeção, implementação e condução do controle interno e na avaliação de sua eficácia

Não existe sistema e processo considerado infalível. A empresa e seus gestores devem estar cientes que risco zero nunca vai existir, a não ser que a organização não faça ou pratique a operação no seu mercado. A inerência do risco sempre irá existir.

O grande desafio no desenvolvimento da ISO 31000 estava em estabelecer uma linguagem comum, bem como padronizar as melhores práticas e abordagens para que as organizações possam implementar a gestão de riscos em seus processos.

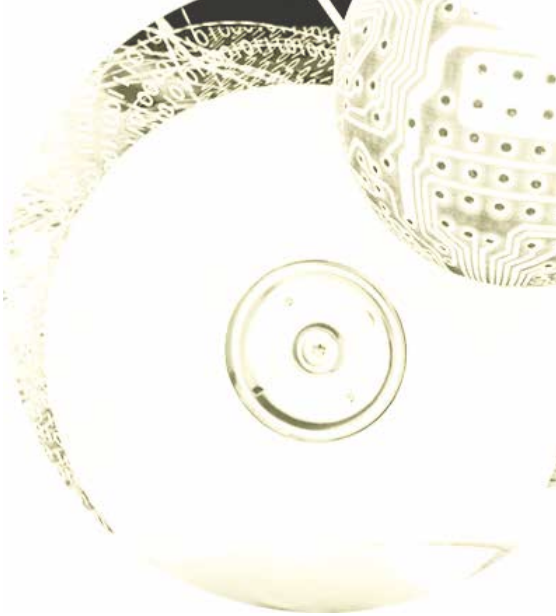
Por se tratar de uma proposta de convergência alinhada com a visão integrada de ERM (Enterprise Risk Management), a ISO 31000 não concorre com outras orientações já existentes, fornecendo orientações e alinhamento com outros conjuntos de regras específicos.

Referências

COSO 2013 - Committee of Sponsoring Organizations of the Treadway Commission - Internal Control - Integrate Framework.

COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management.

ABNT NBR ISO 31.000:2009 - Gestão de Riscos - Princípios e Diretrizes.



Capítulo 5

Fases do Processo de Gestão de Riscos Corporativos

A partir da perspectiva do saber fazer, neste capítulo você terá os seguintes objetivos de aprendizagem:

- ✓ Compreender a concepção do Processo de Gestão de Riscos Corporativos - Método Brasiliano - Avançado.

- ✓ Analisar a abrangência e aplicação do Processo de Gestão de Riscos Corporativos - Método Brasiliano - Avançado, descrevendo as fases do Framework, específico para Risco no processo.

Contextualização

Este capítulo visa abordar o processo de Gestão de Riscos Corporativos, Método Brasiliano - Avançado, possui o *Framework* adaptado da ISO 31000, porém todo o seu conteúdo, o como fazer com métricas e ferramentas, possui os fundamentos integrados do COSO I e II e da ISO 31000, utilizando ferramentas e técnicas da ISO 31010.

Fases do Processo de Gestão de Riscos Corporativos - Método Brasiliano

O processo de Gestão de Riscos Corporativos, Método Brasiliano - Avançado, possui o *Framework* adaptado da ISO 31000, porém todo o seu conteúdo, o como fazer com métricas e ferramentas, possui os fundamentos integrados do COSO I e II e da ISO 31000, utilizando ferramentas e técnicas da ISO 31010.

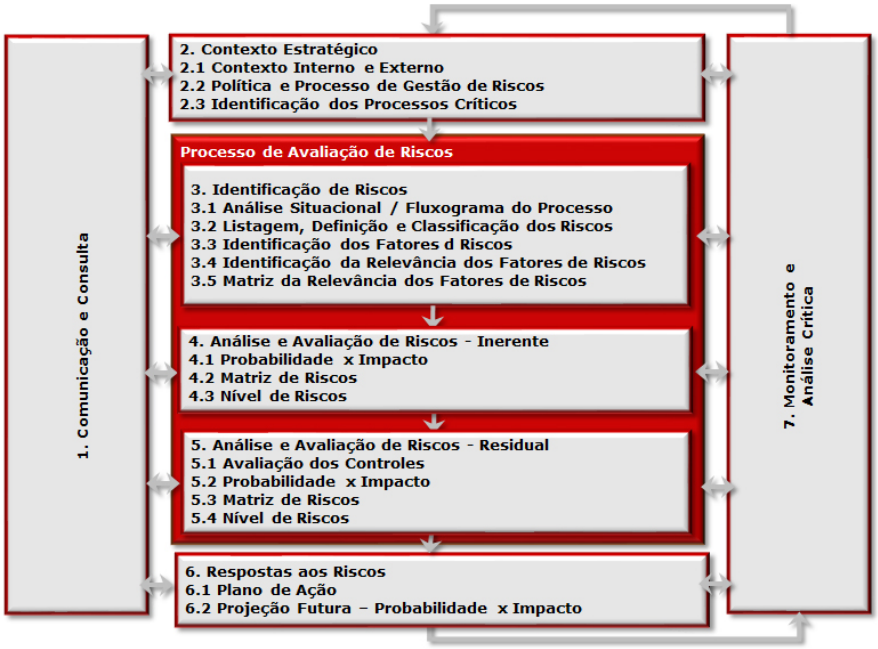
Optamos por um *Framework* integrado tendo em vista nossa experiência de mercado, nestes 28 anos de experiência, em identificar que as três estruturas (COSO I, II e ISO 31000) possuem suas características próprias, mas juntas consideramos imbatíveis em termos de abrangência e cobertura em todas as disciplinas.

A “cara” do *framework* foi adaptada da ISO 31000 porque o processo de comunicação e consulta é muito mais profundo e abrangente, possuindo uma filosofia de sensibilização e capilarização em toda a organização, e seus usuários através de programas de *endomarketing*, além é claro, de dar também relevância com os relatórios para todas as partes interessadas. O processo de Gestão de Riscos Corporativos, Método Brasiliano - Avançado, possui sete fases conforme descrito abaixo:

- Fase 1 - Comunicação e Consulta
- Fase 2 - Contexto Estratégico
- Fase 3 - Identificação de Riscos
- Fase 4 - Análise e Avaliação de Riscos - Inerente
- Fase 5 - Análise e Avaliação de Riscos - Residual
- Fase 6 - Respostas aos Riscos
- Fase 7 - Monitoramento e Análise Crítica

Abaixo *framework* com os principais elementos do Processo de Gestão de Riscos Corporativos, Método Brasiliano - Avançado.

Figura 15 - *Framework* do Método Brasiliano



Fonte: Brasiliano (2016, p. 99).

Ressaltamos o emprego da realização da análise do risco inerente, sem levar em consideração os controles e ou sistemas de segurança, e depois a realização da análise do risco residual.

Nesta fase há necessidade de fazer uma avaliação da eficácia dos controles existentes e operacionalizados para identificar se houve redução da inerência do risco. A ISO 31000 não é enfática neste quesito, sendo que os COSO I e II sempre reforçaram a importância da realização das duas avaliações (inerente e residual).

Descreveremos aseguir, em cada capítulo, as fases do Framework, específico para Risco no processo.

a) Fase 1 - Comunicação e consulta

A comunicação e consulta é importante aspecto a ser considerado em cada fase do processo de gestão e análise de riscos corporativos.

Cabendo desenvolver um plano de comunicação com as partes envolvidas internas e externas, logo no primeiro estágio do processo.

A comunicação envolve diálogo entre as partes envolvidas, tendo como foco a consulta e *não somente a comunicação de via única.*

A comunicação interna e externa eficaz é importante para assegurar que os responsáveis pela implementação da gestão de riscos e os investidores compreendam as bases sobre as quais as decisões são tomadas, e por que determinadas ações são necessárias.

A percepção do risco pode variar em função de diferentes hipóteses, conceitos e necessidades, e de questões e interesses das partes envolvidas, por estarem relacionados ao risco ou aos assuntos em discussão.

As partes envolvidas tendem a julgar a aceitabilidade de um risco baseadas em sua própria percepção do risco.

Uma vez que as partes envolvidas podem ter um impacto significativo nas decisões tomadas, é importante que sua percepção do risco, bem como sua percepção dos benefícios sejam identificadas e documentadas, e as razões subjacentes, compreendidas e abordadas.

Venda Interna da Gestão de Riscos

O profissional de gestão de riscos, auditoria e de segurança necessita entender e saber utilizar os recursos que possui, para poder sobressair e destacar o processo, reforçando as medidas preventivas e proativas.

A venda da gestão de riscos é um trabalho de conscientização dos riscos e de seus controles e sistemas. É um grande desafio para o departamento de marketing e recursos humanos implementar junto com a gestão de riscos um programa eficiente e prático.

É um grande desafio para o departamento de marketing e recursos humanos implementar junto com a gestão de riscos um programa eficiente e prático.

O grande desafio é saber vender que o processo de gestão e análise de riscos corporativos será útil para todos os usuários, pois terão condições de possuir uma visão de antecipação dos possíveis problemas. Com esta visão os colaboradores passam a prospectar cenários de riscos, agindo de forma pró ativa e não somente reagindo aos problemas. Há a necessidade da implementação do *endormaketing* para que possa ser compreendido e haja uma forte colaboração por parte do seu público interno. A venda interna possui três premissas básicas:

1) O público alvo de sua campanha são todos os colaboradores da organização, considerados como cliente interno. Como todo "Cliente", este só pode ser conquistado e retido com um serviço onde haja qualidade;
2) O cliente interno, assim como o externo, possui expectativas e estas devem ser superadas, portanto a gestão de riscos tem de compreender a expectativa e cultura dos colaboradores para realizar um ajuste fino no programa de divulgação;
3) A excelência da operacionalização do processo de gestão e análise de riscos corporativos significa envolver os colaboradores e comprometê-los com os objetivos do Gerenciamento de Riscos.

Essas três premissas trazem como consequência direta o entendimento por parte dos colaboradores do que é a Gestão e Análise de Riscos e sua função. O *endomarketing* passará a estimular o Gerenciamento de Riscos nos seguintes aspectos:

- conscientização da importância na prevenção dos sistemas e processos existentes;
- orientação para o público interno em respeitar normas e procedimentos.

A Gestão de Riscos deve planejar o processo de comunicação como parte integrante da sua Política. O processo de *endomarketing* deve ser realizado em conjunto com o departamento de Recursos Humanos da empresa e *marketing*, pois necessita conhecimento e informação específica do público interno, informações estas que o Recursos Humanos já deve possuir.

Deve-se ter em mente que o treinamento é a principal alavanca do processo de *endomarketing*. O treinamento precisa ser percebido como momento ótimo para o envolvimento do colaborador, para valorizá-lo como pessoa e comprometê-lo com os objetivos da empresa. O treinamento sempre é um investimento com retorno garantido em termos de qualidade, excelência e dedicação.

A empresa que não puder se vender para seu público interno, tampouco venderá para o externo. E isto é muito perigoso em uma época de competitividade agressiva e grande turbulência, como a que estamos vivendo.

Programa de Comunicação

Abaixo um *framework* com as fases de um programa completo de comunicação, que a área de gestão de riscos deve operacionalizar.

Figura 16 - Programa de Comunicação

Fonte: Brasiliano (2016, p. 104).

Um programa transmite confiança e credibilidade, ao mesmo tempo em que os valores compartilhados pela cultura organizacional, irão com certeza incentivar a postura proativa em vez da reativa, assumindo desta forma um papel cada vez mais criativo, sugerindo soluções viáveis e lutando para que toda a organização possa cumprir seus objetivos.

O Processo de Comunicação

Para alcançar os resultados, o processo de comunicação deve permear todo o plano de desenvolvimento de análise de riscos até a fase de instalação do programa e permanecer ativo após seu desenvolvimento. Ele é de tal modo estratégico, que sem a comunicação não poderá existir o processo de gerenciamento de riscos, uma vez que se não houver sensibilização, não haverá a participação necessária e desejada para o desenvolvimento adequado e pleno gerenciamento de riscos.

Para alcançar os resultados, o processo de comunicação deve permear todo o plano de desenvolvimento de análise de riscos até a fase de instalação do programa e permanecer ativo após seu desenvolvimento.

As ações do Plano de Comunicação e Consulta servirão para orientar todos os empregados e equipes e conscientizá-los da importância do processo em relação ao nível de informação que devem absorver e o que devem fornecer aos gestores de risco durante o processo de criação e implantação das políticas. Além disso, deve servir para mantê-los envolvidos diretamente e posteriormente e possam agir corretamente diante de qualquer tipo de ocorrência seja um indício, uma crise ou uma emergência.

Para a alta administração e área de Gestão de Riscos Corporativos, o programa de comunicação deve conter todo o direcionamento para as áreas de negócios da empresa e deve ser entendido e implantado por inteiro, pois seu conteúdo deve contemplar a orientação estratégica do processo de gerenciamento de riscos e da Comunicação de Crises.

Para as demais áreas e empregados, ele deve conter os mecanismos para envolver os funcionários numa ação conjunta que alimentará os grupos que estarão administrando o processo.

Para o público externo, ele deve estar preparado para mantê-los bem informados e harmonizados a fim de que o processo caminhe de modo a receber a compreensão desses públicos e eventualmente, a contribuição que for esperada deles nos objetivos do programa.

O plano de comunicação deve ser estruturado para ser implantado com o público interno e externo

O plano de comunicação deve ser estruturado para ser implantado com o público interno e externo e deve ter os seguintes objetivos:

I - Público Interno

- Orientar e conscientizar o empregado sobre a importância do programa;
- Envolver e comprometer o empregado no processo.

II - Público Externo

- Informar os principais públicos de relacionamento com a empresa sobre o plano de riscos.
- Orientar e conscientizar os representantes dos públicos externos sobre a importância dos riscos.
- Posicionar a empresa no mercado e fortalecer sua imagem corporativa.

O plano de comunicação deve ter três níveis de atuação e desenvolvimento:

- Implantação e acompanhamento do programa de riscos.
- Criação do manual de comunicação de crise.
- Acompanhamento do processo de implantação da Política de Gestão de Riscos.

O procedimento para implantação dos três níveis deve ser feito a partir da criação de uma Campanha de Comunicação, que terá como ações:

- Lançamento do programa;
- Divulgação dos processos e passos de implantação;
- Estudo do ambiente interno;
- Estudo do ambiente externo;
- Criação dos meios de comunicação;
- Implantação dos meios e processos de informação.

Campanha de Comunicação

A empresa deve considerar primeiro o lançamento interno da campanha, já que se trata de público estratégico e prioritário, uma vez que ele é agente de integração e colaboração no processo.

A campanha pode utilizar os recursos existentes de comunicação interna e também criar outros que forem necessários e adequados para transmitirem a mensagem do programa. Os principais meios e veículos de comunicação a serem utilizados são:

- Intranet, infos eletrônicos, blogs, twitters, vídeocast e podcasts;
- E-mails, e-mails-marketing, filmes e vídeos ilustrativos e educativos;
- Folders, banners, cartazes, jornal interno, revista e jornal mural.

A campanha deve ser dirigida a todos os empregados, prestadores de serviço, parceiros da empresa e desenvolver a disseminação das informações de forma geral, vertical e horizontal.

Redes de Comunicação

Além da campanha por meio dos veículos, que disseminará todas as informações, a equipe de comunicação deve também desenvolver processos de relacionamento com a implantação de redes de comunicação, preparando empregados de departamentos para serem agentes de comunicação, propagadores e coletores de informações, a fim de levarem as informações às equipes e colegas de trabalho e também trazerem feedback para o comando da equipe e do programa.

Grupos de Comunicação

Do mesmo modo que as redes, os grupos funcionam para serem articuladores das informações, agindo de maneira organizada em grupos de discussão e debates em torno dos temas que envolvem o programa. Os integrantes do grupo, após as reuniões temáticas, passam a ter a função de disseminadores das informações em suas áreas e equipes de trabalho.

Essa atividade é de extrema importância para o desenvolvimento do programa e seus objetivos porque tem a característica de disseminar as informações em todo o ambiente da empresa para estimular os demais empregados à participação efetiva no programa.

Já as ações específicas, que fazem parte do processo de consulta, deverão tratar objetivamente os temas do programa e terem como meta levantar com detalhes as informações pesquisadas pelos consultores para alimentar o programa de gestão de riscos. Para que alcancem os resultados desejados e de maneira rápida, essas ações devem ser desenvolvidas e dirigidas aos grupos definidos como estratégicos, que atuarão diretamente no processo de levantamento de informações e consulta.

Para essas ações específicas, a equipe de comunicação deve desenvolver, com os grupos selecionados, atividades como encontros, seminários e workshops. Essas atividades têm a finalidade de envolver o empregado e fazê-lo vivenciar os temas que estão sendo tratados.

- **Seminários**: Alguns assuntos e casos deverão ser discutidos em maior profundidade. Para isso devem ser criados e organizados seminários temáticos, que devem ir desde as filosofias e princípios organizacionais como visão, missão e valores e políticas e diretrizes organizacionais permeando os temas desenvolvidos pelo programa de gestão de riscos.

- **Workshops**: Outros assuntos técnicos que precisam ser compreendidos em profundidade com seus respectivos procedimentos devem ser tema e objeto de workshops dirigidos às chefias, técnicos, gerentes e diretores.

As Redes e Grupos de Comunicação, os Seminários e Workshops deverão ter como objetivo transferir informações orientadas para que sejam discutidas em profundidade e analisadas de acordo com a experiência de cada integrante a fim de que passem a fazer parte da rotina de cada um de seus integrantes. Assim, de modo geral devem ser considerados os seguintes aspectos:

- Além das orientações gerais comuns, cada empregado deve conhecer profundamente as orientações especificas de sua área, dos grupos de risco e dos seus riscos específicos.

- Devem conhecer também os procedimentos e medidas gerais e as diferenças entre planos de emergência, contingência e comunicação e suas ações específicas por grupo e tipo de risco.

Plano de Comunicação - Continuidade do Processo

Visando manter a continuidade do plano de comunicação, a empresa deve considerar outros formatos, sendo:

- **Campanha Dirigida**: O processo de comunicação deve ser contínuo mesmo após o período de levantamento de informações, ou seja, de comunicação e consulta. Para isso, a empresa deve criar uma campanha dirigida com os temas propostos pelo Processo de Gestão de Riscos. Essa campanha deve ser desenvolvida com os seguintes processos:

- **Campanha de Comportamento**: A campanha será estruturada para ser desenvolvida em três conceitos:

I - Valores

Deve ser o primeiro conceito a ser discutido com todos os empregados para que eles entrem e façam uma imersão do ambiente cultural da empresa. As conclusões e resultados do debate deverão ser divulgados da mesma forma e por meio dos mesmos mecanismos de comunicação da campanha de Comunicação e consulta.

II - Comportamentos Organizacionais

A segunda fase será aplicada com a realização de encontros e seminários semanais com grupos de específicos funcionários e terão como temas a serem conhecidos e debatidos os tópicos definidos pela Política de Gestão de Riscos.

- BIA - Business Impact Análises - Matriz de Processos
- Identificação de Riscos, Fatores e Controles; Fluxograma Riscos no Processo
- Diagrama de Causa e Efeito; Matriz SWOT
- Análise e Avaliação de Riscos - Matriz e Nível Riscos

- Plano de Ação
- Risco Assumido; Monitoramento do Risco.

Com a análise desses temas permeando os seminários, os grupos terão oportunidade de avaliar os comportamentos organizacionais e compreender as atitudes praticadas à luz da cultura e políticas organizacionais.

III - Proteção

O debate entre os grupos deverá caminhar para a análise ponderada dos melhores comportamentos que, baseados nos critérios da Gestão de Riscos, levarão a empresa, a partir das atitudes individuais e de grupos, assegurar um ambiente de permanente controle dos riscos e, em função disso, altamente protegida contra os riscos corporativos existentes.

Etapas do Programa

I - Campanha de Comunicação

- Iniciar a campanha com divulgação de **Teasers** baseados na ‘construção do processo.
- Despertar a curiosidade das pessoas sobre o tema.
- O teaser será seguido de campanha com peças como: Cartazes, Banners, Terminal de Consulta, Intranet, Volantes Explicativos, Matérias no Jornal Interno, vídeos.

Durante os primeiros dias, a coordenação da campanha deverá criar “Quiz” sobre os temas a serem abordados e disponibilizados nos meios de comunicação interna.

II - Treinamento Líderes

Durante o período de lançamento da campanha, realizar Encontro de toda liderança estratégica.

Essa atividade tem como finalidade alinhar o conhecimento da liderança sobre a Gestão de Riscos, pois as lideranças integrantes desse grupo serão responsáveis pela execução das atividades seguintes. O encontro terá como formato:

- Abordagem conceitual e estratégica
- Abordagem técnica e prática

Esse trabalho existe também para ressaltar a importância do Líder no processo, como também para prepará-los para o relacionamento e para serem multiplicadores dos princípios e tópicos da Gestão de Riscos.

III - Imersão e Sensibilização

Os líderes realizam reuniões e encontros com suas equipes e tratam de temas divulgados pela campanha interna, informando que serão organizados encontros para aprofundamento dos temas e assuntos da Gestão de Riscos.

IV - Encontros e Seminários

Os líderes serão responsáveis por realizarem encontros / seminários com suas equipes. Os encontros serão em número suficiente para alcançar todo o grupo liderado. Dessa forma, toda a empresa será envolvida e participará do processo de discussão. Os Encontros deverão ter abordagem conceitual, estratégica e prática e serem realizados com ações de envolvimento com dinâmicas e vivências, analogias e cases. Basicamente desenvolverá o estudo dos valores e da cultura organizacional, os comportamentos e os princípios da Gestão de Riscos. O conceito chave dos encontros deverá ser o mesmo do conceito geral:

Conhecimento, Comportamento e Proteção

Central de Informações

Durante todo o período de realização da campanha, a área de comunicação da empresa, além de participar das atividades, deverá fazer o devido acompanhamento do processo e criar as condições necessárias para que os grupos e todos os funcionários recebam regularmente informações sobre o programa e possam também se manifestar e buscar esclarecimentos sobre tudo o que está acontecendo, como informações sobre o programa, atividades, participação, etc.

Para isso, a área de comunicação deverá montar uma Central de Informações, que terá como objetivo coordenar o desenvolvimento das ações de comunicação e fazer o controle de todo o processo. A Central de Informações deverá servir como um canal permanente de disseminação e recepção de informações.

A Central de Informações será coordenada e gerenciada pela área de comunicação da empresa e orientada e supervisionada por um comitê formado por representantes das demais áreas, com prioridade para as áreas de Auditoria e Administração.

A Central de Informações funcionará por meio da coordenação de um profissional que será o coordenador de comunicação do programa e dos grupos e redes de comunicação. Ele deverá fazer atendimento pessoal e por meio um canal direto como telefone (ramal fixo e celular) e-mail e virtual pela intranet da empresa. Desse modo, qualquer funcionário que desejar se comunicar para esclarecer ou tirar dúvidas a respeito do processo ou ainda encaminhar sugestões ou críticas, poderá fazê-lo por meio desses canais.

Grupo de Atuação Permanente

O grupo de atuação permanente tem como objetivo observar, avaliar e manter o processo implantado da Gestão de Riscos presente na mente das pessoas e entre os grupos e departamentos. Ele estará a postos sempre que uma determinada necessidade surgir em qualquer área ou departamento da empresa. Sempre que houver qualquer tipo de necessidade ou ocorrência, o grupo deverá:

- Orientar os colaboradores e contratados sobre os procedimentos a serem observados e mantidos.
- Manter os funcionários da empresa informados sobre o status da situação geral.
- Acionar os meios internos, por área, para avaliar e tomar a decisão necessária quando for necessário.

O grupo de atuação deverá ser formatado da seguinte maneira:

- Cada área deverá indicar um membro que fará parte do grupo.
- O grupo deverá se reunir mensalmente para avaliar as condições de cada área e trocar informações sobre os fatos e acontecimentos, em especial, sobre a manutenção de tudo o que foi discutido durante a fase de comunicação dos riscos.

Recomendações finais sobre a implantação da filosofia e plano de comunicação

Em linhas gerais, o processo que deverá ser seguido no momento do lançamento da campanha, seja o da "Comunicação e Consulta" ou da "Comunicação Dirigida", devem levar em conta as seguintes fases:

- Definir o tema geral da campanha e a estrutura para a necessidade do momento;
- Preparar o cronograma de atividades e as fases de avaliação e revisão;
- Preparar as peças definidas para o lançamento – criação e produção.

O "*teaser*" deve ser divulgado alguns dias antes do lançamento da campanha. Nesse momento, os grupos de comunicação iniciam seu trabalho de relacionamento com os demais funcionários visando estimular as discussões sobre o que foi divulgado na forma do *teaser*.

O grupo deve manter esse clima por uns dois ou três dias. Durante esse período, a equipe de comunicação deve soltar um e-mail ou colocar uma informação adicional nos meios de comunicação internos para estimular a curiosidade.

No dia do lançamento, a empresa deve amanhecer com os cartazes e banners todos colocados e inicia-se a campanha com informações mais detalhadas do tipo: como e o que é a campanha, seus objetivos, atividades, etc.

Nesse dia pode-se fazer um evento, café da manhã, almoço, um grande encontro ou encontros menores por áreas, por exemplo. Os veículos como o blog, jornal, quadro mural vão sendo utilizados com informações que vão alimentando as atividades e os debates sobre os temas definidos no roteiro do programa.

Os grupos de comunicação começam a fazer as reuniões, outras ações vão sendo implementadas de acordo com a evolução do programa.

As avaliações e correções de rumo devem ser realizadas periodicamente, pelo menos a cada semana.

b) Fase 2 - Contexto Estratégico

Ao estabelecer o contexto, a organização articula seus objetivos e define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelece o escopo e os critérios de risco para o restante do processo. Portanto temos três contextos a serem definidos e alinhados:

1) O Contexto Empresarial - Interno e Externo;
2) O Contexto de Gestão de Riscos - Metodologia e Critérios.
3) Identificação dos Processos Críticos

1. Contexto Empresarial - Ambiente Interno e Externo

Ambiente Interno

A primeira etapa diz respeito a compreensão dos objetivos estratégicos e organizacionais da empresa, compreendendo sua cadeia de valor e respectivos

Fatores Críticos de Sucesso. É importante que a área de gestão de riscos esteja alinhada com os objetivos estratégicos da empresa, seguindo as premissas da ISO 31000 e do COSO II, entendendo suas políticas, objetivos, missão, valores e estratégias implementadas na organização. Com base na missão estabelecida, a administração planeja objetivos principais, seleciona as estratégias e estabelece outros planos a serem adotados por toda a organização, alinhados com a estratégia e a ela vinculados. Embora muitos objetivos sejam específicos a uma determinada organização, alguns deles são amplamente compartilhados. Por exemplo, os objetivos comuns a praticamente todas as entidades são alcançar e manter uma reputação favorável tanto no segmento empresarial quanto com seus clientes, fornecer informações confiáveis às partes interessadas e operar em conformidade com as leis e a regulamentação. A área de gerenciamento de riscos deve estar alinhada com todas estas premissas estratégicas da organização, por esta razão do entendimento estratégico da empresa.

A ISO 31000 (2009, p. 15) discorre sobre o ambiente interno das empresas o seguinte:

O contexto interno é algo dentro da organização que pode influenciar a maneira pela qual uma organização gerenciará os riscos. Convém que ele seja estabelecido, por que:

a) a gestão de riscos ocorre no contexto dos objetivos da organização;
b) convém que os objetivos e os critérios de um determinado projeto, processo ou atividade sejam considerados tendo como base os objetivos da organização como um todo, e
c) algumas organizações deixam de reconhecer oportunidades para atingir seus objetivos estratégicos, de projeto ou de negócios, o que afeta o comprometimento, a credibilidade, a confiança e o valor organizacional.

É necessário compreender o contexto interno. Isto pode incluir, mas não está limitado:

- à governança, estrutura organizacional, funções e responsabilidades;
- às políticas, objetivos e estratégias implementadas para atingí–los;
- às capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
- aos sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais);
- às relações com as partes interessadas internas, e suas percepções e valores.
- às normas, diretrizes e modelos adotados pela organização, e
- à forma e extensão das relações contratuais.

Para isso sugerimos que o gestor disponha de um checklist com o objetivo de melhor identificar as variáveis que compõem o contexto empresarial. A seguir uma sugestão genérica, a título de exemplo:

1) A Empresa atua em qual segmento? Quais são os seus produtos e/ou serviços?
2) Atualmente, qual é a posição que da Empresa ocupa no ranking de seu segmento de atuação?
3) Quais são os concorrentes diretos da Empresa? E os indiretos?
4) Quais são os fornecedores chave para da Empresa?
5) Quais são os objetivos estratégicos de médio prazo?
6) A Empresa dispõe de Código de Conduta ou outras políticas relativas às práticas de negócio (valores éticos)?
7) Os colaboradores conhecem e entendem a(s) política(s) existentes na Empresa?
8) A Empresa pratica alguma política de incentivo para atingir suas metas? Ex.: Bônus para colaboradores.
9) Há algum meio de monitoramento que tenha por finalidade verificar a efetiva prática da(s) política(s) existente(s) na Empresa?
10) Atualmente, qual é a estrutura organizacional da Empresa? (Organograma).
11) O Organograma geral atende às necessidades de negócio da Empresa? Caso não, qual a necessidade que julga necessária e por quê?
12) Considerando a estrutura organizacional apresentada quais são as áreas consideradas como “áreas chave” e respectivas atividades críticas em termos de faturamento?
13) A Estrutura Organizacional da Empresa é descentralizada, semi-integrada ou de sistema integrado?

Abaixo figura ilustrativa do entendimento do contexto interno e externo:

Figura 17 - Contexto Externo e Interno

Fonte: Brasiliano (2016, p. 125).

Ambiente Externo - Cenários

O contexto externo é o ambiente externo, onde estão inseridas as variáveis incontroláveis. Entender o contexto externo é importante para entender quais são as variáveis que podem dificultar ou expor os objetivos estratégicos da organização e entender as interconectividades entre as variáveis incontroláveis. O contexto externo pode incluir, mas não está limitado a:

- O ambiente cultural, social, político, legal, regulamentar, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local;
- Os fatores-chave e as tendências que tenham impacto sobre os objetivos da organização;
- As relações com as partes interessadas externas e suas percepções e valores.

Podemos exemplificar os componentes do contexto externo:

- Localização física da empresa: posição geográfica da instalação (rios, estradas, elevação, condições climáticas, etc.);
- Configuração socioeconômica da área em que a empresa está instalada (população vizinha, status social, área urbana/rural, instalações policiais);
- Situação político-financeira do país (legislação pertinente, identificação e análise dos órgãos que legitimam, planos governamentais e política econômica e financeira);

A gestão de Riscos poderá buscar a informação destas variáveis, de maneira direta ou indireta, através de duas fontes:

- Fontes Primárias: São as fornecidas no ambiente da empresa (troca de informações)
- Fontes Secundárias: Fornecidas pelos órgãos governamentais (colaboração integrada).

O nível de detalhamento e profundidade dependerá da necessidade e da influência do impacto sobre a empresa.

A natureza do ambiente muda com muita rapidez, conduzindo a alterações políticas e sociais. Esta rapidez exige da empresa capacidade impressionante de resposta e adaptação. Como exemplo de problemas ambientais externos, podemos citar:

- Há previsões de recessão econômica, no país, o que aumentará o desemprego. Qual será a influência deste fato sobre a empresa? Aumentam as possibilidades de saque, furto, roubo, mudança de relacionamento? A empresa está preparada para receber este impacto?
- As condições climáticas podem afetar a empresa? Ela está preparada para reagir a uma inundação? Existe plano de emergência com esta finalidade?
- Uma guerra pode ocorrer proximamente no Oriente Médio? Qual o impacto na minha empresa, uma multinacional, que apoia a intervenção militar? Há possibilidade de sabotagem ou ameaça de bomba?

Estas indagações devem ser analisadas e seu impacto para a empresa projetado. A gestão de riscos abrange toda a conjuntura ambiental, devendo avaliar todos os seus ângulos.

Nesta fase pode–se empregar a ferramenta de construção de cenários utilizando a Matriz de Impactos Cruzados para entender a motricidade das variáveis externas nos objetivos estratégicos.

2. Contexto da Gestão de Riscos - Metodologia e critérios

O contexto da gestão de riscos diz respeito à estrutura organizacional da área, ou seja, como que a empresa pretende gerenciar seus riscos, quais serão os critérios e metodologias a serem utilizadas. Isto tudo deve estar formalizado nos documentos: Política de Gestão de Riscos, que fornece as diretrizes estratégicas; e no Processo de Gestão de Riscos, que fornece a metodologia com todo os critérios, descrevendo com detalhe como realiza a gestão de riscos.

A ISO 31000 descreve que o contexto do processo de gestão de riscos irá variar de acordo com as necessidades de cada organização. Ele pode envolver, mas não está limitada:

- à definição das metas e objetivos das atividades de gestão de riscos;
- à definição das responsabilidades pelo processo e dentro da gestão de riscos;
- à definição do escopo, bem como da profundidade e da amplitude das atividades da gestão de riscos a serem realizadas, englobando inclusões e exclusões específicas;
- à definição da atividade, processo, função, projeto, produto, serviço ou ativo em termos de tempo e localização;
- à definição das relações entre um projeto, processo ou atividade específicos e outros projetos, processos ou atividades da organização;
- à definição das metodologias de avaliação de riscos;
- à definição da forma como são avaliados o desempenho e a eficácia na gestão dos riscos;
- à identificação e especificação das decisões que têm que ser tomadas, e
- à identificação, definição ou elaboração dos estudos necessários, de sua extensão e objetivos, e dos recursos requeridos para tais estudos. A atenção para estes e outros fatores pertinentes pode ajudar a assegurar que a abordagem adotada para a gestão de riscos é apropriada às circunstâncias, à organização e aos riscos que afetam a realização de seus objetivos.

Critérios de Risco

Convém que a organização defina os critérios a serem utilizados para avaliar a significância do risco. Os critérios devem ser definidos no início de qualquer processo de gestão de riscos e sejam analisados criticamente de forma contínua.

O processo a ser escolhido depende das características da empresa, não se limitando, especificamente a nenhuma métrica e ou metodologia. A ISO 31000 cita os seguintes aspectos:

- a natureza e os tipos de causas e de consequências que podem ocorrer e como elas serão medidas;
- como a probabilidade será definida;
- a evolução no tempo da probabilidade e/ou consequência(s);
- como o nível de risco deve ser determinado;
- os pontos de vista das partes interessadas;
- o nível em que o risco se torna aceitável ou tolerável, e se convém que combinações de múltiplos riscos sejam levadas em consideração e, em caso afirmativo, como e quais combinações convém que sejam consideradas.

O ideal é a definição clara e objetiva através de um documento estruturado, que deve ser a Política de Gestão de Riscos, sendo recomendado que a empresa tenha dois documentos:

- Uma Política, onde contém as diretrizes da diretoria e ou conselho, já determinando quem é o dono dos riscos e a estrutura apropriada (Modelo de Política de Gestão de Riscos);
- Um processo descrito com detalhe sobre a metodologia a ser utilizada pela empresa, contendo os seguintes tópicos:

1. Objetivos
2. Definições e Conceitos dos termos a serem utilizados
3. Descrição do Processo de Gestão e Análise de Riscos

3.1 Identificação dos Riscos – Ferramenta

3.2 Análise e Avaliação dos de Riscos Inerentes – Critérios de Probabilidade e Impacto, Matriz e Nível de Riscos

3.3 Análise e Avaliação dos Riscos Residuais – Avaliação dos Controles, Critérios de Probabilidade e Impacto, Matriz e Nível de Riscos

4. Respostas aos Riscos
5. Priorização das ações
6. Monitoramento e Auditoria
7. Anexos - Dicionários de Riscos - Conceituação dos riscos que a empresa irá utilizar

Modelo de Política de Gestão de Riscos

Objetivo

Estabelecer princípios e diretrizes chaves que pautam a atuação da empresa nas questões de Riscos Corporativos.

Campo de Aplicação

Esse procedimento aplica-se à todas unidades de negócio e áreas corporativas da empresa.

Princípios

A Política de Gestão de Riscos Corporativos da empresa possui um processo de Gestão e Análise de Riscos e está baseado em práticas nacionais e internacionais, utilizando o conceito de gestão retro-alimentativa, ciclo do PDCA com monitoramento do sistema de gestão por indicadores e verificação por análise crítica, gerando melhoria contínua.

Este processo deve ser conduzido pelos gestores da empresa e respectivos colaboradores, aplicado no estabelecimento de estratégias formuladas para identificar, em todas as áreas, eventos em potencial, capazes de afetar tanto os objetivos estratégicos como os operacionais, e administrar os riscos para mantê-los compatíveis com o apetite definido, e possibilitar garantia razoável do cumprimento dos objetivos da Empresa.

Compromissos

Por meio desta Política de Gestão de Riscos Corporativos a empresa, estabelece como compromissos:

- Proporcionar um ambiente saudável e seguro às pessoas, patrimônio e operações;
- Atender aos requisitos dos produtos e serviços, mitigar os riscos com impactos significativos aos processos, ao meio ambiente, bem como os perigos e riscos no trabalho, patrimônio, riscos de fraude e informações, atendendo à legislação e outros requisitos subscritos que se relacionem a operação;
- Prevenir a poluição do ar, da água e do solo, e destinar adequadamente seus resíduos;
- Promover a melhoria contínua do desempenho do Sistema de Gestão de Riscos Corporativos;
- Garantir a interação entre os envolvidos disponibilizando informação por meio de eficazes canais de comunicação;
- Obrigações em cumprir as leis e regulamentos locais, nacionais e internacionais, normas e políticas interna, aplicáveis aos seus negócios;

- Treinar, conscientizar e desenvolver a competência em gestão de riscos dos empregados;
- Incentivar a aplicação de tecnologias na melhoria continua dos aspectos de riscos nas suas instalações e operações; e
- Fornecer condições para que a Gerência de Riscos Corporativos possa contribuir com a empresa de forma a alcançar com sucesso sua missão e atingir sua visão.

A Política de Gestão de Riscos Corporativos ajuda os gestores a tratar com eficácia as incertezas, mitigando riscos, a fim de melhorar a capacidade de alcançar os objetivos da empresa. O reconhecimento dos riscos em processos, fraude, patrimoniais, ambientais, de informações, pessoais, trabalho e de atendimentos legais, fator inerente no processo decisório, requer que a administração analise as informações em relação aos ambientes interno e externo, utilize seus recursos, bem como ajuste as atividades frente aos riscos levantados e analisados.

Processo de Gestão de Riscos

O Processo de Gestão de Riscos Corporativos da empresa possui como base o Framework da Norma ISO 31000 - Gestão de Riscos.

A empresa não admite riscos no quadrante vermelho e nível de risco no nível 3 e 4, são considerados como inaceitáveis devendo possuir ações para tratamento por parte dos gestores. Caso não ocorra a resposta ao risco dentro do prazo estimado para tratamento deste, a pendência existente será encaminhada ao Diretor da área para providências.

A empresa não admite riscos no quadrante vermelho e nível de risco no nível 3 e 4, são considerados como inaceitáveis devendo possuir ações para tratamento por parte dos gestores.

Risco Assumido

O risco é assumido quando o Diretor da área responsável pelo processo ou atividade decide assumir, tendo em vista relação custo benefício ou por questões estratégicas, no entanto, é contra a Política de Riscos empresa a possibilidade de assumir riscos no quadrante vermelho e nível de risco 3 e 4.

Revisão do Processo de Gestão de Riscos

As áreas da empresa devem revisar seus riscos, através do Processo de Gestão de Riscos Corporativos descritos nesta política, sempre que necessário ou em um período máximo de doze meses, com o objetivo de monitorar os riscos e os fatores de riscos do ambiente interno e externo.

A implementação do plano de ação da área será monitorada quinzenalmente pela área de Gestão de Riscos Corporativos.

Responsabilidades e Autoridades

Os responsáveis envolvidos na gestão de riscos corporativos são:

I – Diretores;
II – Comitê de Gestão de Riscos;
III – Gerência de Riscos Corporativos;
IV – Gestores;
V – Auditoria Interna;
VI – Facilitadores das Análises de Riscos Corporativos;
VII – Funcionários / Colaboradores.

I – Diretores

- Analisar e decidir sobre o(s) risco(s) a ser(em) assumido(s) pela empresa;
- Inserir os itens de monitoramento previstos neste documento nas Reuniões de Performance das áreas sob sua gestão;
- Indicar participantes para compor o Comitê de Riscos, a fim de acompanhar e apoiar o Processo de Gestão de Riscos Corporativos, evitando possíveis conflitos de interesse na empresa;
- Garantir o cumprimento dos Planos de Ação das áreas sob sua responsabilidade, tomando providências quanto ao não cumprimento das ações dentro do prazo previsto;
- Disponibilizar recursos necessários para o Sistema de Gestão de Riscos Corporativos;
- Apoiar e incentivar o compromisso com o Processo de Gestão de Riscos Corporativos;
- Participar das reuniões análises críticas anuais das Análises de Riscos das unidades sob a sua responsabilidade, bem como verificar o cumprimento das recomendações / sugestões efetuadas.

II – Comitê de Gestão de Riscos

- Acompanhar a gestão integrada de riscos, validando e revisando periodicamente a matriz de riscos da empresa, assim como a estrutura de controles internos capazes de minimizar a ocorrência de riscos;
- Dar apoio às ações para o tratamento dos riscos, alocando recursos para tal fim e reportando-os à Diretoria Executiva e aos Conselhos de Administração e Fiscal;

- Avaliar o desempenho dos indicadores de riscos, de modo a alinhá-los aos objetivos estratégicos da empresa;
- Prover o alinhamento de assuntos estratégicos e operacionais no processo de gestão integrada de riscos;
- Reportar à Diretoria e Conselhos de Administração e Fiscal os resultados do processo de gerenciamento dos riscos;
- Revisar a Política de Gestão de Riscos.

III – Gerência de Riscos Corporativos

- Apoiar o Comitê de Riscos;
- Implementar e gerenciar o Sistema de Gestão de Riscos Corporativos, assegurando a execução dos processos de forma eficaz;
- Assessorar e orientar as áreas da empresa, visando à divulgação e a aplicação das práticas do Processo de Gestão de Riscos Corporativos em todas as suas unidades;
- Manter permanente diálogo com todas as unidades da empresa, apoiando a melhoria contínua do Processo de Gestão de Riscos Corporativos;
- Assegurar que as estruturas de controles e gestão de riscos funcionem efetivamente;
- Avaliar o estado atual da gestão de riscos, fornecendo uma visão que auxilie a administração a identificar atuais e futuros riscos e oportunidades associadas;
- Analisar a performance de gerenciamento de riscos determinada pela empresa;
- Verificar se o tratamento dos riscos e o nível organizacional tratado pela empresa estão adequadamente endereçados;
- Aprimorar a eficiência na gestão de riscos;
- Direcionar a priorização dos riscos considerando a possibilidade de retorno, promovendo a alocação de recursos para o tratamento de riscos associados ao aumento do valor agregado aos acionistas;
- Fornecer conhecimento e habilidades técnicas para o tratamento de riscos-chave;
- Participar no desenho e na definição de controles internos, bem como dar suporte na condução e na interpretação de avaliações dos riscos;
- Reportar as ações preventivas e contingenciais;
- Investigar as alegações de impropriedades cometidas pelos empregados, ou contra a Empresa.

Esse papel diferencia a Gerência de Riscos Corporativos, uma vez que ela não tem responsabilidade de estabelecer e dirigir as operações do negócio e o seu foco primário é monitorar e aprimorar a eficácia das atividades de gestão dos riscos na empresa.

IV – Gestores

- Gerir, implementar e manter atualizada a Análise de Riscos nas áreas e nos contratos sob sua responsabilidade nos termos deste documento;
- Validar as Análises de Riscos e o plano de ação referente, das áreas sob sua responsabilidade;
- Repassar para o Diretor responsável pela área, o(s) Risco(s) que não puder(em) ser eliminado(s) ou reduzido(s), para a análise de Assumir o(s) Risco(s);
- Indicar facilitador responsável pelas Análises de Riscos das áreas sob sua responsabilidade;
- Manter seu pessoal capacitado na realização das Análises de Riscos e cientes dos critérios de criticidade/significância e priorização dos cenários avaliados;
- Coordenar as análises críticas anuais das Análises de Riscos da unidade sob a sua responsabilidade, bem como verificar o cumprimento das recomendações / sugestões efetuadas;
- Garantir o cumprimento das ações estabelecidas em plano de ação dentro dos prazos programados, das áreas sob sua responsabilidade;
- Inserir os itens de monitoramento do Processo de Gestão de Riscos Corporativos nas suas Reuniões de Performance com equipe e Diretoria;
- Assegurar à Diretoria os recursos necessários (financeiros, humanos, materiais e de sistema) para propiciar o gerenciamento efetivo dos riscos identificados nas áreas e nos contratos sob sua responsabilidade;
- Atender e seguir as diretrizes e procedimentos da empresa relacionadas à contratação e gestão de fornecedores e contratadas.
- Os gestores da empresa são responsáveis pela detecção e prevenção de fraude. Qualquer membro do time gerencial deve estar alerta para qualquer indicação de irregularidade dentro de sua área de responsabilidade. Em adição, tem a responsabilidade de reportar imediatamente os atos suspeitos para o Gestor de Riscos Corporativos, não devendo tentar conduzir pessoalmente investigações, entrevistas ou interrogatórios.

O não cumprimento das ações previstas no Plano de Ação dentro do prazo estabelecido será informado ao Diretor responsável da área para as devidas providências, a fim de decidir sobre Evitar, Assumir ou Reduzir o(s) Risco(s) a níveis aceitáveis.

v – Auditoria Interna

- Auditar os controles visando avaliar o funcionamento efetivo através de testes por amostragem dos riscos nos processos, fraude, físicos,

patrimoniais, ambientais, de informações, saúde e segurança do trabalho;
- Auditar os atendimentos legais os quais serão identificados no processo de Gestão de Riscos Corporativos.

VI – Facilitadores de Análise de Riscos Corporativos

- Compartilhar ao seu gestor da empresa mudanças ou propostas de mudanças na organização, em suas atividades ou materiais;
- Compartilhar ao seu gestor da empresa as modificações no Processo de Gestão de Riscos Corporativos, incluindo mudanças temporárias, bem como seus impactos nas operações, processos e atividades;
- Comunicar e treinar a unidade nas análises de riscos, das áreas sob sua responsabilidade;
- Acompanhar a implementação das ações previstas no plano de ação oriundas das análises de riscos, das áreas sob sua responsabilidade;
- Inserir os itens de monitoramento nas Reuniões de Performance da equipe e com o gestor empresa;
- Informar nas suas Reuniões de Performance, ou quando necessário, ao gestor das áreas sob sua responsabilidade sobre as ações não cumpridas ou cumpridas em atraso do(s) Plano(s) de ação, assim como pontos que possam comprometer o Processo de Gestão de Riscos Corporativos;
- Apresentar os resultados das análises de riscos e o plano de ação ao gestor;
- Atualizar as análises de riscos, das áreas sob sua responsabilidade, sempre que necessário;
- Conduzir as análises de riscos da unidade nos termos deste documento;
- Controlar toda a documentação relativa às análises de riscos da unidade ou área.

VII – Funcionários / Colaboradores

- Conhecer as análises de riscos da sua unidade de trabalho;
- Cumprir as ações, sob sua responsabilidade, previstas no Plano de Ação dentro do prazo estabelecido;
- Participar dos programas e campanhas da empresa relacionadas ao tema;
- Comunicar qualquer desvio ou ação de melhoria que possa existir nas análises de riscos.

Todos os funcionários têm a responsabilidade de relatar suspeitas que têm ou informações a eles fornecidas sobre a possibilidade de atividades fraudulentas ou corruptas por parte de qualquer executivo, funcionário, fornecedor ou qualquer outra parte associada à empresa. Qualquer pessoa que possui embasamento

razoável para acreditar que atos fraudulentos ou corruptos tenham ocorrido, tem a responsabilidade de reportar imediatamente os atos suspeitos e não deve tentar conduzir pessoalmente investigações, entrevistas ou interrogatórios.

Fraude e Corrupção

A empresa tem tolerância zero à prática e à ocultação de atos fraudulentos ou ilegais. Alegações de tais atos serão investigados até sua conclusão lógica, incluindo ações legais, processos criminais e ações disciplinares onde houver garantia.

A equipe da Gestão de Riscos Corporativos tratará com confidencialidade toda informação recebida e protegerá a reputação dos questionados, restringindo o acesso a toda informação relacionada às alegações e à investigação somente àqueles que legitimamente necessitam ter conhecimento. Onde uma investigação concluir que a ocorrência de um ato fraudulento é provável, o Gerente de Gestão de Riscos Corporativos informará ao gestor superior da natureza a possível extensão das atividades.

Considerações Gerais

Documentos referenciados:

- ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário.
- ABNT NBR ISO 31.000:2009 – Gestão de Riscos – Princípios e Diretrizes.
- ABNT NBR ISO 31.010:2012 – Gestão de Riscos – Técnicas para o Processo de Avaliação de Riscos.

Termos e Definições

- **Funcionários / Colaboradores:** todos aqueles que possuem vínculo empregatício.
- **Facilitadores:** representantes das áreas indicados pelos gestores, responsáveis pelas Análises de Riscos de suas áreas.
- **Gestores:** ocupantes de cargo de liderança, tais como Gerentes, Coordenadores e Supervisores que tenham equipes sob sua gestão.

Registro da Operação

Identificação	Armazenamento	Proteção	Recuperação	Tempo de Retenção	Descarte
	Software				

Histórico das Revisões

Data da Revisão Anterior	Data da Revisão Atual	Elaborador	Alterações
-	26/05/16	Brasiliano & Associados / Gestão de Riscos	Emissão inicial

3. Identificação dos Processos Críticos

O BIA - Business Impact Analysis, ou Análise de Impacto no Negócio é uma ferramenta que possibilita avaliar processos, áreas ou atividades e inseri-los dentro de uma escala de criticidades visualizada através de uma Matriz.

O objetivo de realizar o BIA, em primeiro lugar, é de o gestor enxergar qual é o processo/atividade/área considerada crítica ou estratégica para a empresa e montar o seu plano de implantação ou de priorização para começar a gestão de riscos. Esta ferramenta vale para toda e qualquer tipo de disciplina de riscos, segurança corporativa, por exemplo, passa a enxergar qual área dentro da empresa a segurança tem que colocar maior foco de atuação. Em termos de processos, os gestores de cada departamento passam a visualizar quais processos são considerados estratégicos para o negócio. Desta maneira podem colocar maior foco, dar maior atenção, alocar mais recursos na diminuição e mitigação dos riscos. É uma ferramenta que veio da área de tecnologia da informação, com o objetivo de identificar quais sistemas deveriam ter prioridade em termos de *backup*, prioridade para entrar em funcionamento, entre outros. A ISO 31010, Técnicas e Ferramentas de Análise e Avaliação de Riscos, selecionou o BIA para ser empregado na seleção de consequências/impacto. O BIA, tradicionalmente na área de TI, é empregado com dois critérios: o do impacto e do tempo de retorno da operação (quanto tempo a empresa aguenta ficar sem o sistema?). Com base nestes critérios temos condições de elaborar uma escala de criticidade de sistemas.

Utilizado dois macros critérios (impacto e tempo), já mundialmente utilizados pelo BIA e implementado dentro de cada macro critério outros parâmetros com o objetivo de montar uma matriz em três níveis.

Como resultado temos uma escala de processos/atividades/áreas considerados estratégicos e ou críticos para o negócio, podendo o gestor de cada área e o próprio gestor de riscos saber quais processos devem ser monitorados de forma mais constante.

Portanto o BIA é uma ferramenta estratégica e holística no processo de gestão de riscos, pois direciona cada gestor, como se fosse uma bússola, para pilotar, monitorar os processos realmente essenciais.

Critérios do BIA

Para a análise de Impacto no Negócio são utilizados dois critérios de avaliação:

a) **Impacto no Negócio:** Qual impacto na empresa, que a inatividade de um determinado processo ou determinada área provocam? Vejam que a pergunta sempre está voltada para a empresa, nunca para o departamento ou gerência. O impacto tem que ser medido com o foco nos objetivos estratégicos da empresa. Para a avaliação do Impacto no Negócio são utilizados 4 subcritérios sendo eles: Imagem, Financeiro, Legal e Operacional.

b) **Tempo de Tolerância:** Tempo de tolerância é o tempo máximo que um processo, atividade ou área estudada podem ficar paralisados sem comprometer de forma significativa as operações da empresa.

- **Avaliação do Impacto no Negócio:** Para avaliar o impacto no negócio da empresa, os gestores deverão utilizar um peso diferenciado para cada subcritério, tendo em vista o nível de importância no contexto da empresa. Segue abaixo os quatro subcritérios com os respectivos pesos:

Figura 18 - Critérios do Impacto do BIA

Fonte: Brasiliano (2016, p. 143).

Cada subcritério de impacto possui os seguintes critérios para pontuação. Estes critérios nas tabelas podem mudar, de acordo com as características de cada empresa. Segue abaixo:

Quadro 1 - Critérios de Impactos

Imagem	Pontuação
Repercussão prolongada ou não na mídia internacional: Possível boicote aos serviços, manifestações de massa. Preocupação pública/da mídia/ política nacional e internacional. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para reações de sindicatos de trabalhadores e de rede sociais e possíveis greves de funcionários. Impacto sobre o preço das ações/avaliação de crédito. Viabilidade financeira ameaçada. Repercussão internacional no ambiente organizacional.	05
Repercussão nacional: Preocupação pública/ da mídia/ política nacional. Repercussões junto a autoridades governamentais e representantes de nível nacional e/ou regional; possibilidade de medidas restritivas à organização. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão nacional no ambiente organizacional.	04
Repercussão regional: Preocupação pública/da mídia/política dentro do estado. Pode haver envolvimento adverso de grupos de ação e/ ou do governo local. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão local no ambiente organizacional.	03
Repercussão local: Envolve algum interesse público local do munícipio e/ou alguma atenção política local e/ou mídia local, com possíveis aspectos adversos para as operações. Repercussão limitada no ambiente organizacional.	02
Sem repercussão: Situações nas quais não há o conhecimento do público, mas não existe interesse público. A ocorrência não ultrapassa os limites internos da organização e/ou de suas unidades.	01

Financeiro	Pontuação
Catastrófica: Acima de R$ 300.000,00	05
Crítica: De R$ 150.000,00 a R$ 300.000,00	04
Grave: De R$ 100.000,00 a R$ 150.000,00	03
Moderada: De R$ 50.000,00 a R$ 100.000,00	02
Leve: Até R$ 50.000,00	01

Legal	Pontuação
Catastrófica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo descumprimento nos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos indenizações, havendo também possibilidade da suspensão das atividades da empresa, prisão de empregados. Uma ou múltiplas ações judiciais e multas de valor alto. Ação judicial muito séria incluindo ações populares. Encerramento legal das operações.	05

Catastrófica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo descumprimento nos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos indenizações, havendo também possibilidade da suspensão das atividades da empresa, prisão de empregados. Uma ou múltiplas ações judiciais e multas de valor alto. Ação judicial muito séria incluindo ações populares. Encerramento legal das operações.	05
Crítica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo descumprimento dos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos indenizações.	04
Graves: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo pequenas falhas nos procedimentos ou legislação e ainda em que há argumentos e provas para inibir parcialmente a aplicação de multas ou pagamentos indenizações.	03
Moderada: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, porém há argumentos e provas contundentes para inibir a aplicação de multas ou pagamento de indenizações.	02
Leve: Questões legais sem qualquer impacto.	01

Operacional	**Pontuação**
Massivo: Impacta outros processos muito fortemente.	05
Severo: Impacta outros processos de forma direta.	04
Moderado: Impacta levemente outros processos.	03
Leve: Impacta somente o próprio processo.	02
Insignificante: Não impacta nada.	01

Fonte: Brasiliano (2016, p. 144 a 146).

Determinação do Nível de Impacto: O Nível de Impacto é o resultado da média ponderada dos quatro critérios de impacto (multiplicação do peso versus a nota dividido pela soma dos pesos), conforme demonstrado abaixo:

$$\text{Nível de Impacto} = \frac{\text{Imagem} + \text{Financeiro} + \text{Operacional} + \text{Legislação}}{\text{11 (soma dos pesos 4+3+2+2)}}$$

O resultado do nível de impacto é a tabela a seguir.

Grau de Impacto	Escala	Nível de Impacto
4,51 - 5,00	5	Massivo
3,51 - 4,50	4	Severo
2,51 - 3,50	3	Moderado
1,51 - 2,50	2	Leve
1,00 - 1,50	1	Muito leve

- **Avaliação do Tempo de Tolerância:** Como parte da avaliação do impacto, temos que estimar por quanto tempo o processo, atividade ou área analisada pode ficar indisponível ("fora do ar"). O importante é avaliar o tempo necessário para que o processo volte a ser operacional, mesmo que em condições precárias. A escala de valoração para a tolerância de tempo é a seguinte:

Tempo em Horas	Pontuação
Até 4 horas	6
Até 1 Dia – 24 horas	5
Até 2 Dias – 48 horas	4
Até 7 Dias – 168 horas	3
Até 14 Dias – 336 horas	2
Mais de 14 Dias – 336 horas	1

Matriz de Processos Críticos - BIA - Business Impact Analysis

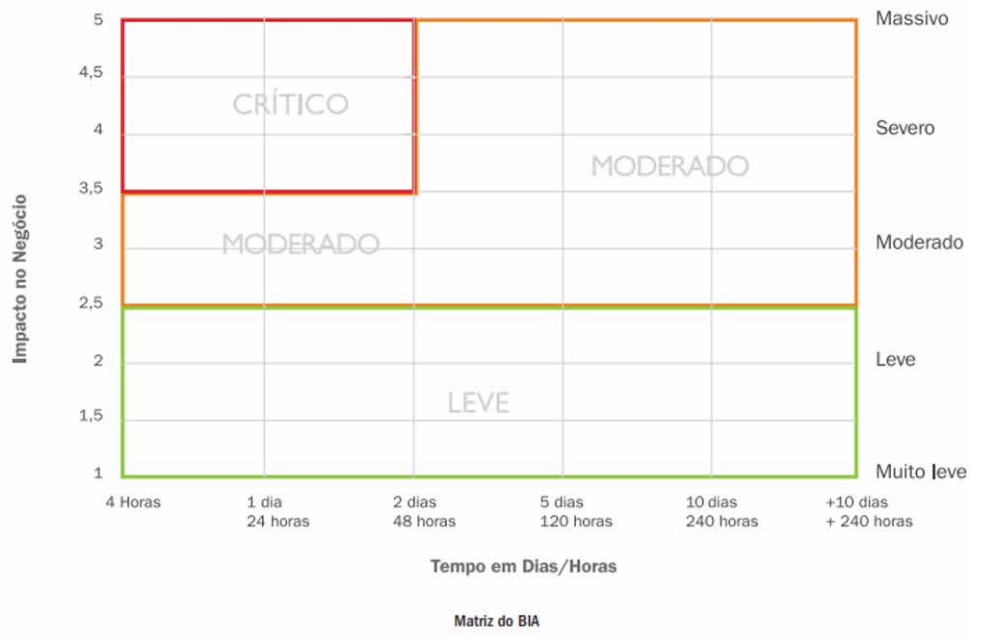
O resultado do cruzamento do nível de impacto com o nível de avaliação da tolerância ao tempo é uma matriz, que define o nível de criticidade de cada processo/atividade/área, o que determina a escala Crítico, Moderado e Leve. Com base nesta matriz o gestor pode determinar a prioridade de implantação, monitoração e alocação de recursos. Temos então três níveis de classificação:

Quadro 2 - Níveis de Prioridade

Críticos (Hot)	Moderados (Warm)	Leves (Cold)
Prioritário: Não pode parar, é primordial para as operações da empresa e deve possuir uma atenção especial dos gestores.	Segunda prioridade: Possui um nível de importância média para a empresa, devendo cada gestor ter um senso de urgência no tratamento.	Terceira prioridade: Pode ser considerado como suporte para os processos, atividades ou áreas consideradas críticas e moderadas.

Fonte: Brasiliano (2016, p. 148).

Figura 19 - Matriz BIA



Fonte: Brasiliano (2016, p. 149).

Exemplo de BIA de Processos

A titulo de exemplo, segue aplicação do BIA, considerando a mensuração do impacto e tempo de tolerância.

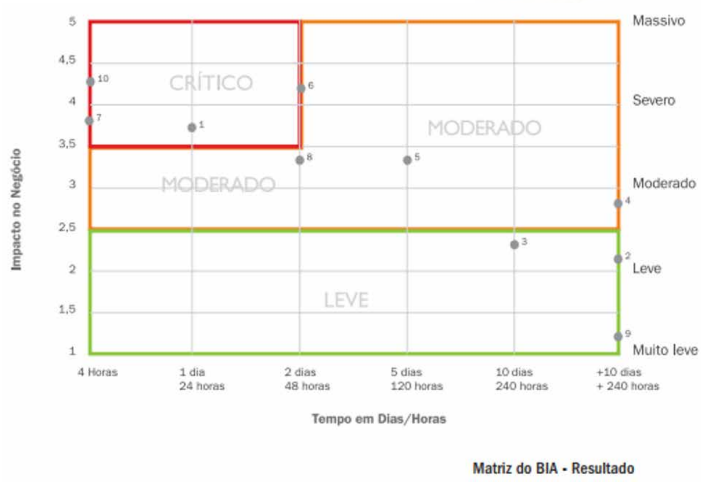
Figura 20 - Listagem e priorização de Processos

Nº	Macroprocesso	Processo	Relevância de Impacto							Tolerância de Tempo	Status
			Imagem	Financeiro	Financeiro	Operacional	Nota	Médioa ponderada de impacto	Nível de impacto	Nível de tolerância	Crítico/ Moderado/ Leve
			4	3	2	2	11	-	-	-	-
1	Administartivo	Contas a Receber	4	5	1	4	41,0	3,73	Severo	5	Crítico
2	Administartivo	Contas a Pagar	3	1	3	1	23,0	2,09	Leve	1	Leve
3	Administartivo	Recursos Humanos	3	1	2	3	25,0	2,27	Leve	2	Leve
4	Administartivo	Marketing	4	2	1	3	30,0	2,73	Moderado	1	Moderado
5	Estoque	Recebimento de Materiais	4	3	2	4	37,0	3,36	Moderado	3	Moderado
6	Estoque	Saída de Materiais	5	4	2	5	46,0	4,18	Severo	4	Crítico
7	Vendas	Vendas de Produtos/ Serviços	4	4	2	5	42,0	3,82	Severo	6	Crítico
8	Compras	Compra de Máteria-prima	4	3	2	4	37,0	3,36	Moderado	4	Moderado
9	Compras	Compra de Materiais de Escritório	1	1	1	2	13,0	1,18	Muito Leve	1	Leve
10	Operacional	Serviço de Mecânica	5	5	1	5	47,0	4,27	Severo	6	Crítico

Identificação dos Porcessos Críticos

Fonte: Brasiliano (2016, p. 150).

Figura 21 - Matriz BIA Preenchida com os processos plotados - Resultado



Cor	Quadrante	Processo
1	Crítico	Contas a Receber
6	Crítico	Saída de Materiais
7	Crítico	Vendas de Produtos/ Serviços
10	Crítico	Serviço de Mecânica
4	Moderado	Marketing
5	Moderado	Recebimento de Materiais
8	Moderado	Compra de Matéria-prima
2	Leve	Contas a Pagar
3	Leve	Recursos Humanos
9	Muito Leve	Compra de Materiais de Escritório

Fonte: Brasiliano (2016, p. 151).

Neste exemplo temos processos listados, sendo que quatro foram considerados críticos, três moderados e três leves. A priorização da implantação do processo de gestão de riscos e o respectivo monitoramento fica sendo para os processos de contas a receber, saída de materiais, vendas de produtos e serviços de mecânica. Nestes quatro processos não poderá ter riscos no quadrante vermelho, pois, em caso de concretização, o impacto será massivo e ou severo, desta forma o gestor - dono do risco (primeira linha de defesa) terá que operacionalizar o processo de gestão de riscos e a área de gestão de riscos (segunda linha de defesa) realizará o monitoramento e a auditoria para verificar se o processo está rodando. Desta forma o ciclo fica abrangente e a empresa protegida.

c) Fase 3 - Identificação de Riscos

A identificação dos riscos possui subfases, todas interligadas e interdependentes, com o objetivo de identificar as principais causas dos riscos versus os processos críticos de cada área.

1. Análise Situacional do Processo: Identificar as Fragilidades e os Controles e Compreender o Histórico

Para possuir uma visão holística e bem acurada dos riscos e de seus fatores de riscos há a necessidade de realizar uma avaliação das condições do processo que estaremos realizando o estudo.

Para possuir uma visão holística e bem acurada dos riscos e de seus fatores de riscos há a necessidade de realizar:

- Uma avaliação das condições de segurança do processo, sendo assim, o gestor deve percorrer o processo, com o objetivo de identificar pontos fortes e fracos, que sirvam de fatores para mitigar ou potencializar a concretização dos riscos. A visão para identificar fragilidades (pontos fracos) deve ser, sempre, pensando como "burlar" os controles existentes. Nessa fase é necessário evidenciar as fragilidades.
- Mapear histórico de ocorrências (caso exista).
- Identificar controles no processo.

Os dados para a análise situacional devem ser extraídos a partir de visitas "in loco", percorrer os processos, através de entrevistas com gestores, análise de fluxograms, normas existentes, seguindo os testes:

- Teste de compreensão: Permite conhecer o funcionamento dos processos e seu fluxo operacional;
- Teste de observância: Permite verificar a realidade das ações que são realizadas/operacionalizadas em termos de controles, normas e sistemas integrados aplicados e utilizados na empresa.

Este estudo das condições deve responder a pelo menos duas perguntas:

- *O que pode acontecer? Lista de riscos.*
- *Como e porque pode acontecer? Causas e Cenários de Riscos.*

Podemos utilizar como referência a ferramenta: 2W 1H - What? Why? How?

O processo de conhecer as condições é um diagnóstico que deve responder a pergunta básica: "qual a situação real do processo quanto aos seus aspectos de controle, frente a sua política de gestão de riscos e aos seus objetivos estratégicos?" Esta 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.

Este contexto, que poderemos chamar de ambiente, varia constantemente e deve ser encarado tanto sob o ponto de vista interno, como externo. Sob o ponto de vista da gestão de riscos a variação permanente do ambiente cria oportunidades ou ameaças à empresa. O diagnóstico corresponde a uma análise, ou uma fotografia e possui duas premissas básicas que devem ser consideradas:

- O ambiente onde o processo está inserido e suas múltiplas variáveis.

- O ambiente proporciona simultaneamente oportunidades que devem ser usufruídas e as ameaças que devem ser evitadas.

A análise do ambiente interno e externo deve ser integrada e contínua. O processo estudado deve ter identificado seus pontos fortes e fracos para enfrentar as diversas situações, sejam contingenciais ou de rotina.

Análise das Variáveis Externas

A análise das variáveis externas tem por finalidade estudar a relação existente entre o processo e seu ambiente, em termos de oportunidades e ameaças. Este estudo inclui, por exemplo, questões como criminalidade, fornecedores, econômicas, entre outros.

Análise das Variáveis Internas

A análise das variáveis internas do processo tem por finalidade evidenciar as qualidades e as deficiências dos processos, controles e sistemas que a corporação possui. A visão para a realização deste diagnóstico deve ser conjuntural, abrangendo todos os segmentos do departamento em que o processo está inserido. Pode-se levar em consideração capacitação, tecnologias, formalização de normas, entre outros.

Quando se inicia o diagnóstico, deve-se ter definido: quais são os processos a serem estudados e quais controles e sistemas estão operacionalizados. Sem estes dois parâmetros é difícil avaliar os pontos fortes e fracos de um sistema e ou processo. Listamos outro checklist na área de processos, a título de exemplo:

1) A Empresa aplica algum meio de conciliação das informações das áreas chave?
2) A Empresa dispõe de unidades de negócio localizadas fora de sua Sede. Elas são convenientemente monitoradas quanto à produção, resultados, ambiente, meios, controles, etc.? Como?
3) A Empresa dispõe de estoque para peças e/ou produtos acabados?
4) Quais são os tipos de controles utilizados pelas áreas chave em suas atividades críticas? (Relatórios, planilhas, etc).
5) A Alta Administração dá a devida atenção aos seus considerados, controles internos?
6) Há uma clara estrutura dos papéis e responsabilidades individuais dos colaboradores no contexto da Empresa? (Descrição de cargos e o que cada um contempla).
7) As equipes das áreas estão bem dimensionadas, considerando inclusive os recursos necessários para a boa execução de suas atividades?

8) Os colaboradores possuem pleno conhecimento de suas atividades (importância, o que fazem; por que fazem)?
9) A Empresa possui programa de Reciclagem/Treinamentos Esporádicos para com seus colaboradores?
10) Caso sim, qual é a frequência?
11) Quais são as ferramentas tecnológicas disponíveis para a execução das atividades da Empresa?
12) Os recursos de TI atuais atendem às necessidades de execução e controle das atividades/operações da Empresa?
13) Existe um plano de treinamento específico para o usuário dos sistemas de informação?
14) Existe um plano de instrução de negócios/recuperação de desastre formalizado?
15) Os sistemas dos aplicativos utilizados atendem às necessidades do processo envolvido?
16) Os sistemas dos aplicativos utilizados são vulneráveis a acessos e alterações de dados?
17) Existem procedimentos formalizados para garantir a segurança da informação?
18) São realizados backups periódicos para as atividades/informações críticas do processo?
19) As informações críticas transmitidas interna ou externamente são criptografadas durante o processo?
20) Existe um responsável de segurança de informação a nível executivo?
21) Existem sistemas e controles específicos para captura de dados relativos a eventos de segurança, incluindo todas as fontes válidas, por exemplo nomes de usuários?
22) Existem procedimentos periódicos de análise desses dados e eventos?

Formas de Realizar um Diagnóstico

A melhor maneira de realizar um diagnóstico é colher as informações em campo, ou seja, olhar o que realmente está acontecendo. Há três maneiras de realizar a busca destas informações:

a) **Entrevistas:** As entrevistas, geralmente nos níveis institucional, intermediário e operacional têm por objetivo conhecer como pensam tanto as pessoas que operam, como os usuários do processo.
b) **Verificação de Documentos:** A verificação de documentos, tais como planos e normas, tem por meta conhecer o que preconizam as condutas e qual é a política de riscos da empresa.

c) **Trabalho de Campo:** O trabalho de campo tem por finalidade comparar se o que está escrito e falado realmente acontece. O ideal é que o diagnóstico possa ser realizado a partir destes três métodos, para garantir uma noção clara e específica das reais condições.

Exemplo de análise situacional voltada para processos:

Figura 22 - Descrição das atividades do processo, identificação dos controles e fatores de riscos

Área	Atividade / Descritivo da Área
Cliente	Atendimento na loja?
Cliente	Sim: acessar a loja para realização do serviço
Vendas	Acessar o sistema e verificar o cadastro do cliente
Vendas	Possui cadastro?
Vendas	Não: realizar o cadastro do cliente no sistema
Vendas	Sim: abrir ordem de serviço?
Vendas	Informar valores de serviços ao cliente
Vendas	Necessário negociar valor?
Vendas	Sim: aplicar valor de desconto parametrizado no sistema
Vendas	Desconto aceito?
Vendas	Sim: imprimir ordem de serviço
Vendas	Não: aplicar desconto de gerente com senha individual
Vendas	Desconto aceito?
Vendas	Sim: imprimir ordem de serviço
Vendas	Não: aplicar desconto fora da alçada sistema

Nº	Controle
C1	Senha e contra senha do gerente regional para desconto

Nº	Fator de Risco
F3	Conluio entre gerente regional e gerente do dia
F7	Ausência das análises de concessões de descontos

Análise Situacional – Processo

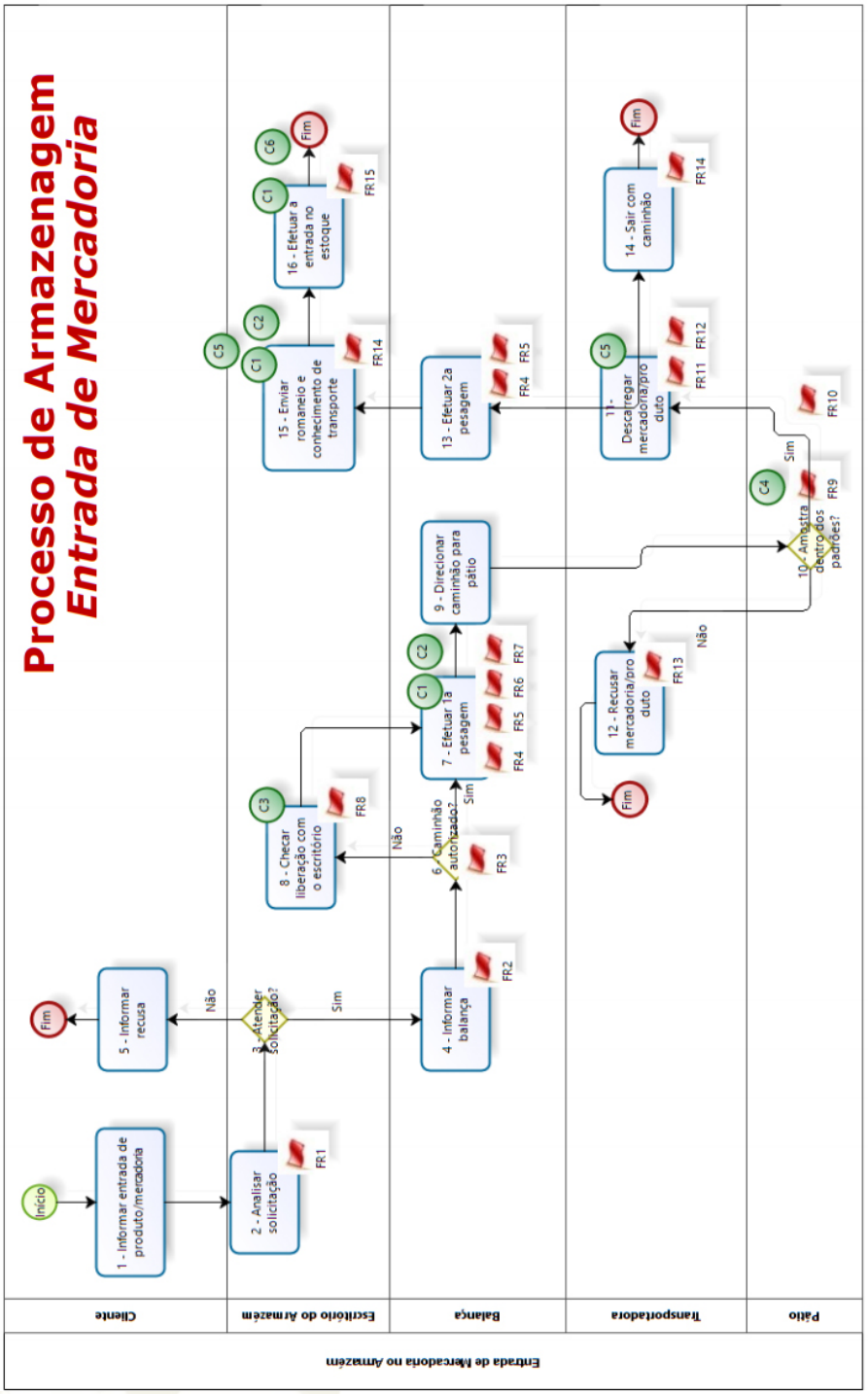
Fonte: Brasiliano (2016, p. 159).

Fluxograma do Processo

O fluxograma é uma ferramenta que permite representar graficamente um fluxo de informações de um processo, percorrendo todas as áreas e atividades.

Após a elaboração do fluxograma do processo é possivel identificar os gaps e controles existentes para cada atividade, melhorando o entendimento das falhas que podem existir em cada atividade. Veja um exemplo de fluxograma:

Figura 23 - Identificação dos controles e fatores de riscos – fragilidades no processo, através do fluxograma



Fonte: Brasiliano (2017).

Figura 24 - Listagem dos fatores de riscos – fragilidades no processo

N	Fator de Risco	N	Fator de Risco
1	271 - Solicitação informal do cliente para entrada do produto	9	279 - Manipulação dos resultados das amostras de qualidade.
2	272 - Ausência de formalização do escritório para balança.	10	281 - Existência de pragas no local de armazenagem.
3	273 - Liberação de entrada dos caminhões através da identificação pessoal do motorista.	11	282 - Conluio entre o descarregamento e o motorista.
4	274 - Recebimento de produto sem aviso do cliente.	12	283 - Ausência de padrão para as informações de recusas dos produtos.
5	275 - Falta de energia no armazém não permitindo o funcionamento da balança.	13	284 - Manipulação do lastro do caminhão pelo motorista.
6	276 - Ausência de nobreak e/ou gerador para a balança.	14	285 - Ausência de integração sistêmica entre a balança (entrada) e o sistema Alfa.
7	277 - Manipulação das divergências de peso entrega.	15	286 - Ausência de tempestividade no registro de entrada de estoque.
8	278 - Ausência de local coberto adequado para as coletas de amostras dos caminhões em dias de chuva.		

Fonte: Brasiliano (2017).

Figura 25 - Listagem dos Controles

N	Controle	Descrição	Objetivo	Tipo	Categoria	Periodici-dade
1	185 - Controle magnético	Dispositivo magnético que fica dentro do armazém para espantar as pombas	Garantir que o controle magnético de pombas funcione, fazendo com que pombas não entrem no armazém	Automático	Preventivo	Sob demanda
2	186 - Confirmação do cliente	Solicitação formal do cliente para o envio da mercadoria para ser armazenada	Garantir que a mercadoria que chegou no armazém para armazenamento, foi realmente enviada pelo cliente para armazenagem	Manual	Preventivo	Sob demanda
3	187 - Validação da nota fiscal de entrada	A nota fiscal acompanha o caminhão quando da entrada do produto, para comprovar origem, nome do cliente, peso, etc	Garantir através da nota fiscal de entrada a origem do produto que está sendo recebido que será armazenado	Manual	Preventivo	Sob demanda

N	Controle	Descrição	Objetivo	Tipo	Categoria	Periodici-dade
4	188 - Ticket de pesagem	controle de pesagem do caminhão (1ª e 2ª pesagem)	Validar o peso do caminhão na 1ª e 2ª pesagem, para a emissão do ticket de pesagem	Automático	Preventivo	Sob demanda
5	190 - Amostra de qualidade do produto entregue	Antes de descarregar o produto, é retirada uma amostra para analisar se o produto está dentro das especificações do armazém	Garantir que todas as mercadorias recebidas, são analisadas e que estão de acordo com os padrões estabelecidos pela empresa, com relação a ph, impureza e umidade	Manual	Preventivo	Sob demanda
6	191 - Registro de estoque	Lançar no sistema de estoque o peso constante no conhecimento de transporte, para o cliente solicitante	Garantir que toda mercadoria que deu entrada no armazém, seja Contabilizada no estoque de produtos armazenados dos clientes	Manual	Detectivo	Sob demanda

Fonte: Brasiliano (2017).

2. Listagem, Definição e Classificação dos Riscos

A listagem deve ser realizada através de reuniões do tipo *brainstorming*, levantando tanto os riscos conhecidos como os desconhecidos. Os riscos desconhecidos são aqueles que nunca aconteceram no contexto da empresa, porém são riscos exequíveis, ou seja, poderão ocorrer.

Técnica do *Brainstorming*

A equipe deverá possuir um líder, visando direcionar os assuntos. Não deve haver censura e nem hierarquia em reuniões deste tipo, visando não inibir a criatividade dos integrantes da equipe. Algumas regras são importantes e devem ser seguidas:

1) Expor as ideias com o máximo de espontaneidade, sem exercer autocensura.
2) Todas as ideias têm interesse, mesmo que pareçam "ideias loucas". São essas, às vezes, as que contêm "algo de novo" e com valor.
3) Nenhuma ideia pode ser contestada ou debatida durante o "brainstorming".
4) Quando um participante tiver uma ideia a apresentar, sugerida por outra já exposta por alguém, terá prioridade sobre os demais.
5) Importante é a quantidade das ideias apresentadas.

Em geral, pela nossa experiência, o número de reuniões pode chegar a três, desde que os participantes da equipe façam suas lições de casa. Estudar as questões relativas aos riscos corporativos de suas empresas. A duração de cada reunião de "*brainstorming*" deve ser no máximo de uma hora e trinta minutos. Além deste tempo, estas ficam ineficazes, sem rendimento.

Ao final das reuniões, deverá haver um consenso, por parte da equipe multidisciplinar, nos riscos levantados.

Após a listagem, os riscos devem ser definidos, e após, classificados, tornando os mesmos aderentes ao negócio da empresa.

A classificação auxilia a organização a ter visão do portfólio dos riscos, na medida em que os agrupa de acordo com suas principais causas. Cabe destacar que a classificação está relacionada à origem/natureza do risco e não ao seu impacto.

Exemplo de listagem de riscos para processo:

Figura 26 - Listagem dos Riscos

N	Risco	Definição
1	121 - Contaminação dos produtos por pragas	O risco está relacionado a existência de pombas no armazém, local onde os caminhões descarregam os produtos, podendo contaminá-los.
2	122 - Manipulação de quantidade recebidas - Fraude	O risco está relacionado a manipulação de divergências de quantidades recebidas (registrando uma carga a menor).
3	123 - Desvio / Roubo de produtos destinados para o armazém	O risco está relacionado ao desvio / roubo de mercadorias durante o trajeto.
4	124 - Recebimento de produtos fora da especificação de qualidade	O risco está relacionado a receber produtos, fora dos padrões estabelecidos pelo armazém, ou seja, um dos itens estar fora do padrão e mesmo assim a mercadoria é aceita para armazenagem.

Fonte: Brasiliano (2017).

3. Identificação dos Fatores de Riscos

Os fatores de risco são, na realidade, a origem e/ou causa de cada evento identificado em cada processo ou área. Para compreender o risco e a soma de todos os fatores identificados, existe a necessidade de dissecar o evento e ou ameaça. O Diagrama de Causa e Efeito (diagrama de Ishikawa ou Espinha de Peixe) é utilizada para o entendimento dos fatores que influenciam a concretização de cada risco.

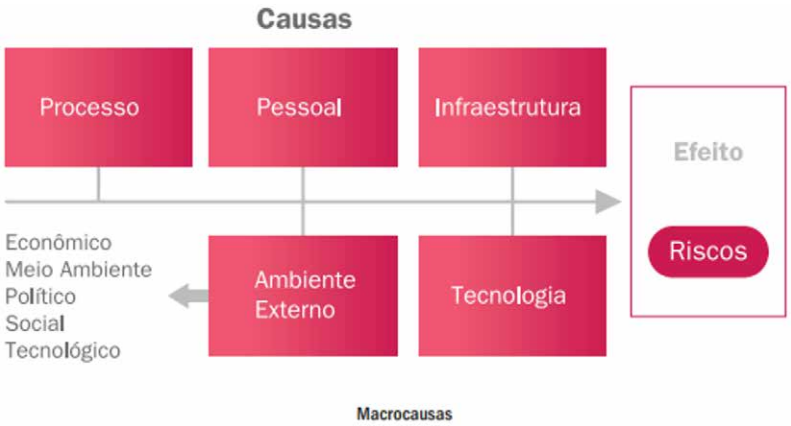
Esta técnica é uma notação simples para identificar fatores que causam o evento analisado. Em 1953 o Professor Karou Ishikawa, da Universidade de Tóquio Japão, sintetizou as opiniões dos engenheiros de uma fábrica na forma de um diagrama de causa e efeito, enquanto eles discutiam problemas de qualidade. O diagrama bem detalhado apresenta a forma de uma espinha de peixe.

Para compreender o risco e o cenário no qual ele está inserido, é importante considerar os diversos fatores que impactam os processos e áreas da empresa. Neste contexto, foi adaptado o diagrama de causa e efeito da qualidade para a área de Gestão de Riscos conforme Macro Causas abaixo:

- **Processo:** Influência da existência de processos, políticas, normas e procedimentos para a materialização do risco.
- **Pessoas:** Influência do nível da equipe envolvida, considerando-se perfil e qualificação, para a materialização do risco, bem como do nível de relacionamento dos colaboradores e da empresa.
- **Tecnologia:** Influência dos sistemas de informação utilizados pela empresa para a materialização do risco.
- **Infraestrutura:** Influência da existência de recursos físicos e sistemas eletrônicos para a materialização do risco.
- **Ambiente Externo:** Influência das variáveis externas incontroláveis para a materialização do risco.

O diagrama de causa e efeito fica exemplificado conforme a seguir:

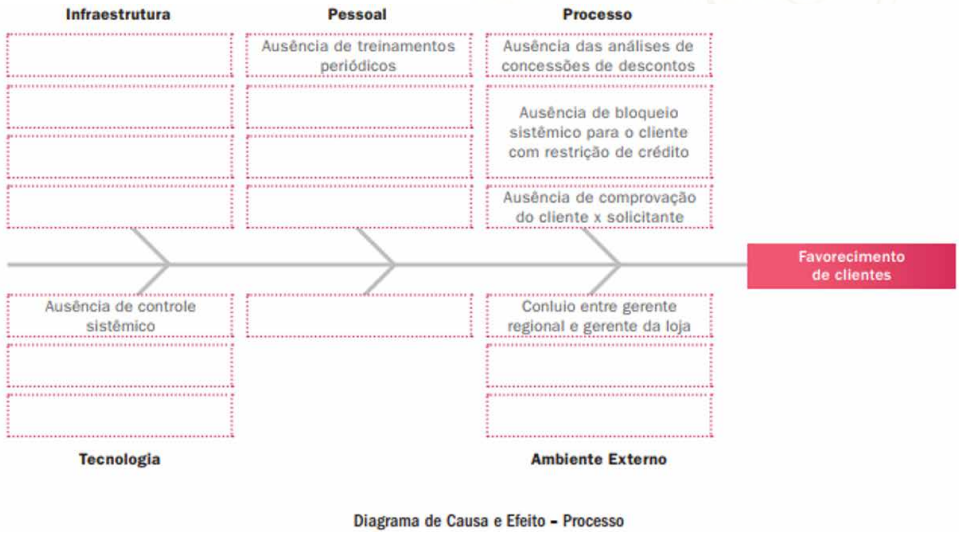
Figura 27 - Diagrama de Causa e Efeito



Fonte: Brasiliano (2016, p. 166).

Ressaltamos que para cada evento identificado existe a necessidade da elaboração de um diagrama de causa e efeito específico. Se estivermos estudando 10 eventos em um determinado processo ou área, teremos que elaborar 10 diagramas de causa e efeito. Exemplo: Favorecimento de Clientes.

Figura 28 - Diagrama de Causa e Efeito – processo



Fonte: Brasiliano (2017, p. 168).

4. Identificação da Motricidade - Matriz SWOT

Após a identificação dos vários fatores de riscos é necessário enxergar estrategicamente quais são os fatores comuns a todos os riscos e quais são os mais motrizes, ou seja, quais são os que podem de fato potencializar os riscos analisados.

Para identificar a criticidade dos fatores de riscos utilizamos a Matriz SWOT, conhecida para identificar os pontos fracos, fortes, oportunidades e ameaças do contexto empresarial. A ferramenta é a Matriz SWOT - FOFA, que em inglês significa Strengths - Weaknesses - Opportunities - Threats e em português - Força - Oportunidade - Fraqueza - Ameaça.

A avaliação das Forças e Fraquezas diz respeito às condições dos nossos controles e nível de operacionalização, são processos que a empresa possui domínio de ação e decisão. São os chamados Fatores de Riscos Internos ou variáveis internas podendo ser negativas (Fraquezas) ou positivas (Forças). Os fatores de riscos considerados incontroláveis dizem respeito à ambiência externa,

podendo ser negativa (Ameaças) ou positivas (Oportunidades). Para identificar a motricidade dos fatores de riscos são utilizados dois critérios de avaliação: Magnitude e Importância.

- Magnitude significa o tamanho ou grandeza que a variável ou evento possui perante o contexto empresarial. Caso aconteça, positivamente 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.

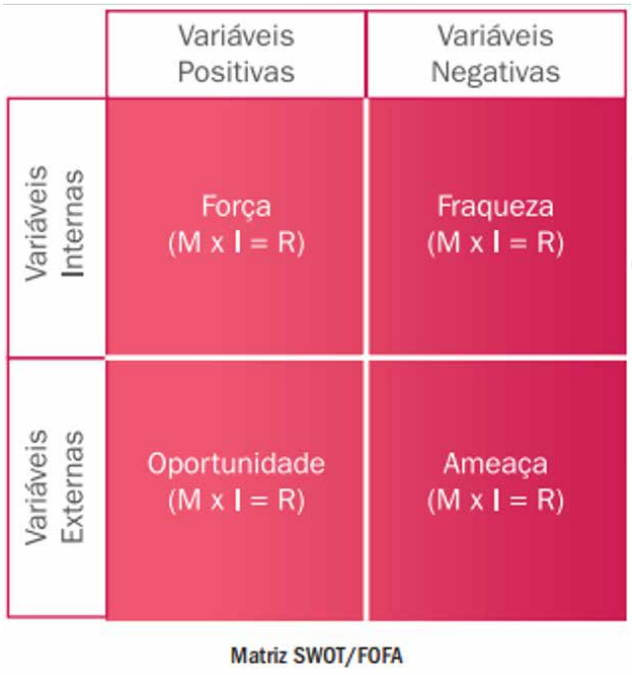
Caso um fator de risco apareça 5 (cinco) vezes em 6 (seis) riscos identificados, significa que esta variável possui **"Alta"** magnitude.

- Importância significa a prioridade que esta 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 (muito importante);
- 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.

Figura 29 - Matriz SWOT/FOFA



Fonte: Brasiliano (2016, p. 70).

A Matriz SWOT/FOFA demonstra o conjunto de fatores de riscos (Fraquezas e Ameaças), e seus pontos fortes e oportunidades. Com esta fotografia o gestor enxergará seus pontos de maior fragilidade. Se formos observar sob o ponto de vista das fraquezas e ameaças contidas na Matriz, podemos afirmar que a Matriz SWOT é um resumo de todos os diagramas de causa e efeito, sem repetir os fatores já listados.

Ponto importante na Matriz SWOT/FOFA, é que as fraquezas são oriundas dos diagramas de causa e efeito, são os resumos dos fatores de riscos que cada área possui. As ameaças são as variáveis incontroláveis do ambiente externo, também oriundas do diagrama de causa e efeito. As variáveis negativas (fraquezas e ameaças) da Matriz SWOT/FOFA são o resumo dos vários diagramas de causa e efeito, sendo a base para a elaboração do Plano de Ação. A Matriz é uma ferramenta de gestão, que possibilita fácil interpretação das principais deficiências e quais são as possibilidades de reversão da situação existente.

A Matriz SWOT/FOFA adaptada para a gestão de riscos permite visualizar o todo, enquanto que o diagrama de causa e efeito visualiza somente o risco analisado.

Figura 30 - Motricidade dos Fatores de Riscos da SWOT - Processo

Fraquezas

ITEM	MAGNITUDE	IMPORTÂNCIA	TOTAL
AUSÊNCIA DAS ANÁLISES DE CONCESSÕES DE DESCONTOS	-2	3	-6
AUSÊNCIA DE BLOQUEIO SISTÊMICO PARA CLIENTE COM RESTRIÇÃO DE CRÉDITO	-2	2	-4
AUSÊNCIA DE COMPROVAÇÃO DO CLIENTE X SOLICITANTE	-1	3	-3
AUSÊNCIA DE CONTROLE SISTÊMICO			
AUSÊNCIA DE PRODUTOS NO ESTOQUE	-2	3	-6
AUSÊNCIA DE TREINAMENTOS PERIÓDICOS	-3	3	-9

Ameaças

ITEM	MAGNITUDE	IMPORTÂNCIA	TOTAL
CONLUIO ENTRE GERENTE REGIONAL E GERENTE DA LOJA	-2	3	-6

Fonte: Brasiliano (2017).

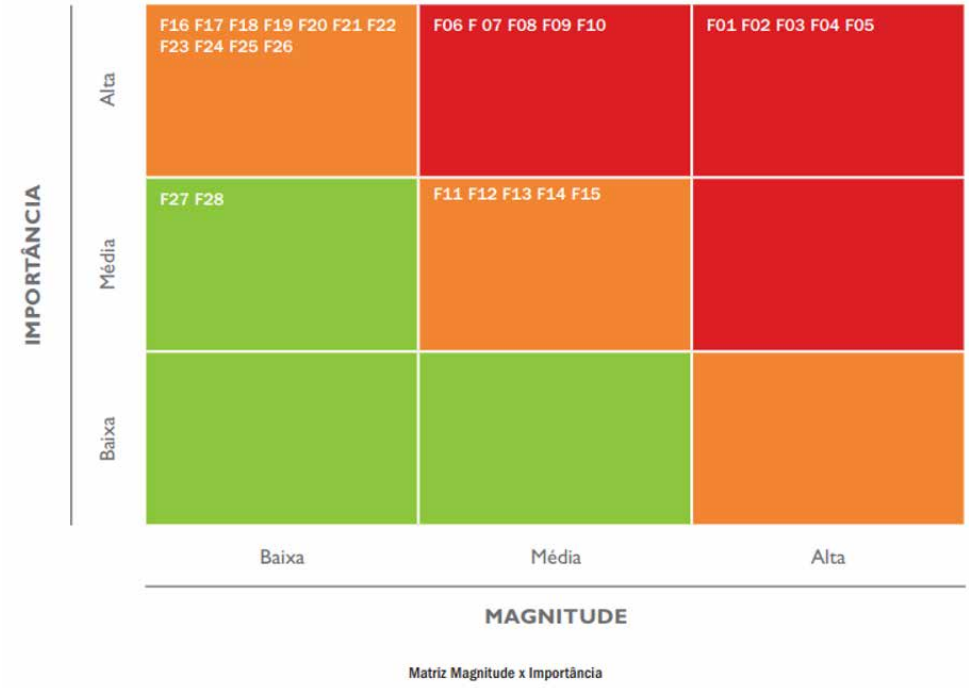
5. Matriz Swot - Magnitude x Importância

Ao observarmos a Matriz SWOT/FOFA acima podemos notar que a prioridade é atribuída levando em consideração o critério das numerações mais altas e negativas, possibilitando que os gestores criem *rankings* para suas ações.

Com base na pontuação de magnitude e importância dada para cada fator de risco de fraqueza, podemos apresentar o resultado em forma de uma matriz que possibilita visualizar a criticidade de cada fator, conforme apresentado abaixo:

O resultado do cruzamento da magnitude com a importância, define o nível de criticidade do fator de risco, ou seja, vermelho, laranja ou verde. Com base nesta matriz o gestor pode determinar a prioridade de tratamento do fator de risco, sempre considerando como primeiro nível o vermelho, segundo nível o laranja é o terceiro nível o verde. A Matriz a ser construída somente com fatores das fraquezas (ambiente interno da empresa).

Figura 31 - Listagem dos Riscos



Fonte: Brasiliano (2016, p. 177).

Fatores de Riscos Comuns

Após a elaboração da Matriz SWOT/FOFA, além da Matriz de Magnitude x Importância é possível também criar um ranking em forma de lista dos fatores de riscos por ordem de criticidade, visualizando os mesmos dos mais críticos aos de menor criticidade.

Figura 32 - Fatores Comuns

CRITICIDADE	FATORES COMUNS
- 9	AUSÊNCIA DE TREINAMENTO PERIÓDICOS
- 6	AUSÊNCIA DAS ANÁLISES DE CONCESSÕES DE DESCONTOS
- 6	AUSÊNCIA DE PRODUTOS NO ESTOQUE
- 4	AUSÊNCIA DO BLOQUEIO SISTÊMICO PARA CLIENTE COM RESTRIÇÃO DE CRÉDITO
- 3	AUSÊNCIA DE COMPROVAÇÃO DO CLIENTE X SOLICITANTE
- 3	AUSÊNCIA DE CONTROLE SISTÊMICO

Fonte: Brasiliano (2017).

d) Fase 4 - Análise e Avaliação de Riscos - Inerente

Entende-se por risco inerente a avaliação dos riscos sem considerar a execução de controles para mitigá-lo.

A análise de riscos visa promover o entendimento do nível de risco e de sua natureza, auxiliando na definição de prioridades e opções de tratamento aos riscos identificados. Por meio dela, é possível saber qual a chance, a probabilidade dos riscos virem a acontecer e calcular seus respectivos impactos nos processos da empresa.

Os riscos são avaliados de maneira qualitativa (subjetiva), ou seja, utiliza critérios pré-estabelecidos com uma escala de valoração para a determinação do nível do risco.

1. Probabilidade x Impacto

A metodologia a ser utilizada para a avaliação de riscos possui dois parâmetros claros a serem analisados:

- Saber qual a chance, a probabilidade, dos riscos virem a acontecer, frente à condição existente de cada processo e área de negócio;
- Calcular o impacto caso seja.

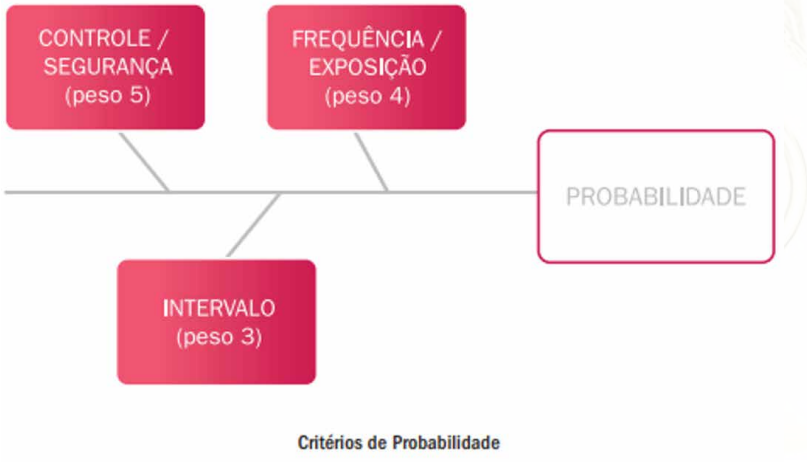
Figura 33 - Probabilidade x Impacto

Fonte: Brasiliano (2016, p. 186).

Determinação do Nível de Probabilidade e Impacto

A probabilidade do risco é calculada através de três critérios, sendo que cada um deles possuirá um peso diferenciado, tendo em vista seu grau de importância. Os critérios de probabilidade são:

Figura 34 - Critérios da Probabilidade



Fonte: Brasiliano (2016, p. 187).

- **Segurança/Controle:** É avaliada a questão dos fatores de riscos e controles identificados na análise situacional. Quanto maior a nota pior é a condição de segurança e dos controles.

Segurança / Controle	
Critério	**Pontuação**
Muito ruim	05
Ruim	04
Média	03
Boa	02
Muito Boa	01

- **Frequência / Exposição:** É a frequência que o risco costuma manifestar-se na empresa ou em empresas similares, podendo levar em consideração históricos internos ou externos (empresas similares).

Frequência / Exposição	
Critério	**Pontuação**
Diário	05
Quinzena	04
Mensal	03
Anual	02
Eventual	01

- **Intervalo:** É avaliada a questão da frequência de avaliação/auditoria e revisão dos controles nos processos, procedimentos e revisão do próprio processo. Quanto maior é o intervalo maior é sua fragilidade.

Intervalo	
Critério	**Pontuação**
Anual	05
Semestral	03
Trimestral	01

O Nível de Probabilidade (Pb) é o resultado da média ponderada dos três critérios de probabilidade (multiplicação do peso vezes a nota dividido pela soma dos pesos), conforme demonstrado abaixo:

$$\text{Nível de Pb} = \frac{\text{Segurança/Controles + Frequência/Exposição + Intervalo}}{\text{12 (soma dos pesos 5 + 4 + 3)}}$$

O nível de probabilidade possui a seguinte classificação:

Grau de Probabilidade	Escala	Nível de Probabilidade
4,51 – 5,00	5	Elevada
3,51 – 4,50	4	Muito Alta
2,51 – 3,50	3	Alta
1,51 – 2,50	2	Média
1,00 – 1,50	1	Baixa

Determinação do Nível de Impacto

Para mensurar o impacto, não devemos levar em consideração somente a questão financeira. Com o objetivo do gestor obter uma visão holística do impacto existe a necessidade de projetar todas as consequências que os eventos causam. Utilizaremos o mesmo critério adotado para identificar o processo crítico. Cada fator de impacto terá um peso diferenciado, tendo em vista seu grau de importância. Cada critério de impacto possui um peso e também uma nota de valoração, tendo em vista o nível de consequência. O objetivo é a obtenção de uma Média Ponderada, equalizando desta forma o Nível de Impacto. Os critérios de impacto são:

Figura 35 - Critérios de Impacto

Fonte: Brasiliano (2016, p. 190).

Cada fator de impacto possui a seguinte tabela:

Quadro 3 - Critérios de Impactos

Imagem	Pontuação
Repercussão prolongada ou não na mídia internacional: Possível boicote aos serviços, manifestações de massa. Preocupação pública/da mídia/ política nacional e internacional. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para reações de sindicatos de trabalhadores e de rede sociais e possíveis greves de funcionários. Impacto sobre o preço das ações/avaliação de crédito. Viabilidade financeira ameaçada. Repercussão internacional no ambiente organizacional.	05
Repercussão nacional: Preocupação pública/ da mídia/ política nacional. Repercussões junto a autoridades governamentais e representantes de nível nacional e/ou regional; possibilidade de medidas restritivas à organização. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão nacional no ambiente organizacional.	04
Repercussão regional: Preocupação pública/da mídia/política dentro do estado. Pode haver envolvimento adverso de grupos de ação e/ou do governo local. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão local no ambiente organizacional.	03
Repercussão local: Envolve algum interesse público local do munícipio e/ou alguma atenção política local e/ou mídia local, com possíveis aspectos adversos para as operações. Repercussão limitada no ambiente organizacional.	02
Sem repercussão: Situações nas quais não há o conhecimento do público, mas não existe interesse público. A ocorrência não ultrapassa os limites internos da organização e/ou de suas unidades.	01

Financeiro	Pontuação
Catastrófica: Acima de R$ 300.000,00	05
Crítica: De R$ 150.000,00 a R$ 300.000,00	04
Grave: De R$ 100.000,00 a R$ 150.000,00	03
Moderada: De R$ 50.000,00 a R$ 100.000,00	02
Leve: Até R$ 50.000,00	01

Legal	Pontuação
Catastrófica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo descumprimento nos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos indenizações, havendo também possibilidade da suspensão das atividades da empresa, prisão de empregados. Uma ou múltiplas ações judiciais e multas de valor alto. Ação judicial muito séria incluindo ações populares. Encerramento legal das operações.	05
Crítica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo descumprimento dos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos indenizações.	04
Graves: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, havendo pequenas falhas nos procedimentos ou legislação e ainda em que há argumentos e provas para inibir parcialmente a aplicação de multas ou pagamentos indenizações.	03
Moderada: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na empresa, porém há argumentos e provas contundentes para inibir a aplicação de multas ou pagamento de indenizações.	02
Leve: Questões legais sem qualquer impacto.	01

Operacional	Pontuação
Massivo: Impacta outros processos muito fortemente.	05
Severo: Impacta outros processos de forma direta.	04
Moderado: Impacta levemente outros processos.	03
Leve: Impacta somente o próprio processo.	02
Insignificante: Não impacta nada.	01

Fonte: Brasiliano (2016, p. 191 a 193).

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

$$\text{Nível de Impacto} = \frac{\text{Imagem} + \text{Financeiro} + \text{Operacional} + \text{Legislação}}{\text{11 (soma dos pesos 4+3+2+2)}}$$

O nível do impacto possui a seguinte classificação:

Grau de Impacto	Escala
4,51 – 5,00	5
3,51 – 4,50	4
2,51 – 3,50	3
1,51 – 2,50	2
1,00 – 1,50	1

Exemplo - Processo:

Figura 36 - Análise de Riscos Inerentes

N º	Macroprocesso	Processo	Riscos	Porbabilidade						Relevância de impacto						
				Frequência / Exposição	Segurança	Intervalo	Nota X Peso	Média ponderada do impaco	Nível de probabilidade	Imagem	Financeiro	Legislação	Operacional	Nota X Peso	Média ponderada do impacto	Nível do impacto
				4	5	3	12			4	3	2	2	11		
1	Vendas	Vendas de produto	Concessão de desconto indevida	3	5	5	52,00	4,33	Muito Alta	3	4	1	3	32,00	2,91	Moderado
2	Vendas	Vendas de produto	Venda sem estoque fisíco	3	5	5	52,00	4,33	Muito Alta	4	4	2	4	40,00	3,64	Severo
3	Vendas	Vendas de produto	Fovorecimento de clientes	4	5	5	56,00	4,67	Elevada	3	4	1	3	32,00	2,91	Moderado
4	Vendas	Vendas de produto	Análise financeira equivocada	2	5	5	48,00	4,00	Muito Alta	3	3	2	5	35,00	2,18	Moderado
5	Vendas	Vendas de produto	Não ser cumprido o prazo de entrega de mercadoria para o cliente	4	5	5	56,00	4,67	Elevada	4	3	3	5	41,00	3,73	Severo

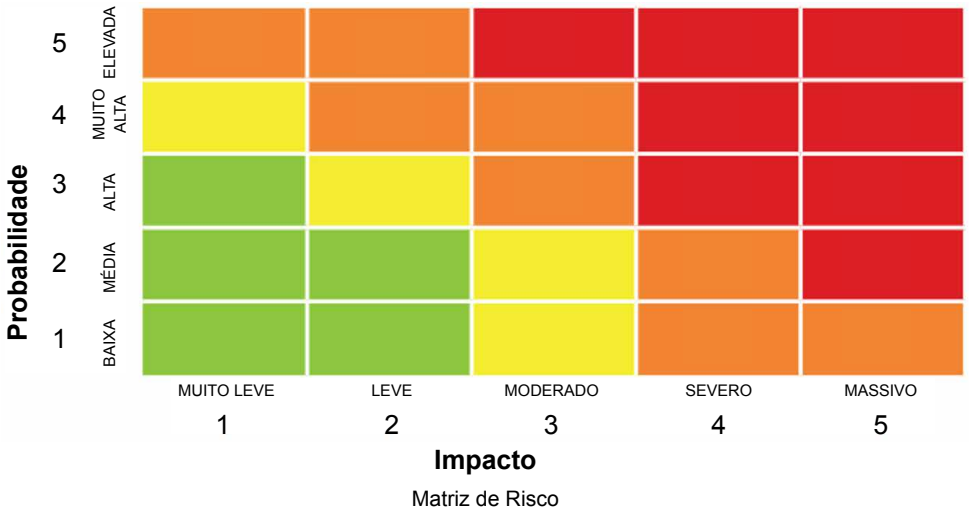
Análise de Riscos Inerentes - Processo

Fonte: Brasiliano (2016, p. 196).

2. Matriz de Riscos

A avaliação de riscos visa comparar os níveis de riscos em relação aos critérios pré-estabelecidos. A relevância dos riscos possui como parâmetro a matriz de riscos e o seu resultado é o grau de criticidade do risco, ou seja, é a priorização que a empresa deve utilizar para tratar cada risco, frente ao seu apetite ao risco. A matriz é dividida em quadrantes e para cada quadrante existe uma estratégia de tratamento e priorização.

Figura 37 - Matriz de Riscos



Matriz de Risco

Fonte: Brasiliano (2016, p. 197).

Para cada quadrante da Matriz de Riscos temos as seguintes classificações e priorizações de tratamento:

- **Quadrante I (Vermelho):** Os riscos existentes no quadrante I são aqueles que têm alta probabilidade de ocorrência e poderão resultar em impacto extremamente severo, caso ocorram. Exigem a implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata. Ações de 0 a 30 dias.

- **Quadrante II (Laranja):** Localizam-se ameaças que poderão ser muito danosas à organização, podendo possuir baixa probabilidade e alto impacto como baixo impacto e alta probabilidade. Estas ameaças devem possuir respostas rápidas, que para isso devem estar planejadas e

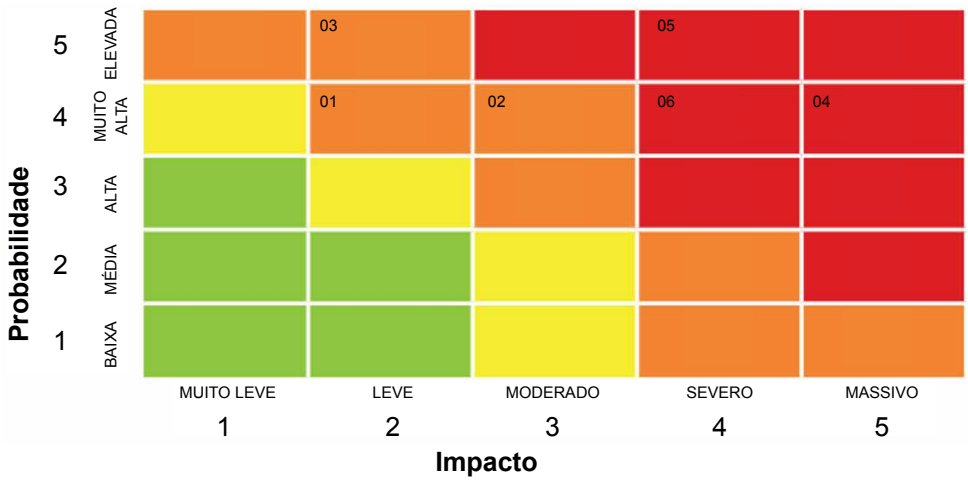
testadas em um plano de contingência, emergência, continuidade de negócios, além de ações preventivas. A diferença do quadrante I é que as ações podem ser implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados. Ações de 0 a 90 dias.

- **Quadrante III (Amarelo):** Localizam-se os riscos com alta probabilidade de ocorrência, mas que causam consequências gerenciáveis à organização. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de emergência. Ponto de monitoramento 1 vez a cada 60 dias.

- **Quadrante IV (Verde):** Os riscos classificados no quadrante IV possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente devem ser gerenciados e administrados, pois estão na zona de conforto. Ponto de monitoramento 1 vez a cada 90 dias.

Exemplo:

Figura 38 - Análise de Riscos Inerentes



Matriz de Risco

Fonte: Brasiliano (2016, p. 199).

3. Nível de Riscos

Após a finalização da etapa para determinar a criticidade de cada risco, deve ser elaborado o Nível do Risco do Processo e/ou Área. O Nível do Risco é um índice que deve ser calculado sempre que houver a avaliação de riscos, geralmente semestralmente, possibilitando mensurar o grau de riscos dos processos ou áreas analisadas, visando facilitar o monitoramento e acompanhamento da evolução dos riscos. Para calcular o Nível de Risco, é necessário utilizar as variáveis já identificadas na etapa anterior de Avaliação de Riscos – Grau de Probabilidade (GP) e Impacto (I), conforme metodologia de cálculo abaixo:

Nível de Risco = Média do GP x Média do I

Para identificarmos o Nível de Risco (Média GP x Média I) é necessário utilizar a tabela de conversão abaixo:

Quadro 4 - Nível de Risco

Nível de Risco	Escala	Quadrante	Tratamento
1 a 5	1	Quadrante IV (Verde)	Áreas ou departamentos que estão na zona de conforto, devendo ser gerenciadas e administradas.
5,1 a 10	2	Quadrante III (Amarelo)	Áreas ou departamentos com algo grau de riscos, mas que causam consequências gerenciáveis à organização. Essas áreas ou departamentos devem ser monitoradas de forma rotineira ou sistemática.
10,1 a 15	3	Quadrante II (Laranja)	Áreas ou departamentos que devem receber tratamento com médio e curto prazo. Possuem cruzamento do grau de risco com médio e grande nível de riscos e elevados impactos. São áreas ou departamentos que devem ser constantemente monitoradas.
15,1 a 25	4	Quadrante I (Vermelho)	Áreas ou departamentos que tem alto grau de risco e poderão resultar em impacto extremamente severo. Exigem implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata.

Fonte: Brasiliano (2016, p. 201).

É importante ressaltar que quanto maior o nível do risco, maior sua criticidade para o processo.

Figura 39 – Nível de Risco

Fonte: Brasiliano (2016, p. 202).

O Nível de Risco é utilizado para determinar seu apetite ao risco, dessa forma, níveis de riscos de processos ou áreas do nível 3 para cima (laranja e vermelho), são considerados intoleráveis. Níveis de riscos que alcancem esses dois quadrantes devem possuir tratamento imediato por parte dos gestores. Exemplo Processo:

Figura 40 - Nível de Riscos Inerentes

RISCOS	PROBABILIDADE	IMPACTO
CONCESSÃO DE DESCONTO INDEVIDA	4,2	2,55
VENDA SEM ESTOQUE FÍSICO	4,6	3,36
FAVORECIMENTO DE CLIENTES	5	2,27
ANÁLISE FINANCEIRA EQUIVOCADA	4,2	2,91
NÃO SER CUMPRIDO O PRAZO DE ENTREGA DE MERCADORIA PARA O CLIENTE	4,6	3,55
TOTAL	**22,60**	**14,64**
MÉDIA	**4,52**	**2,93**
NÍVEL DE RISCOS		**13,23**

NÍVEL DE RISCOS		
1 a 5	1	VERDE
5,01 a 10	2	AMARELO
10,01 a 15	3	LARANJA
15,01 a 25	4	VERMELHO

Fonte: Brasiliano (2016, p. 204).

e) Fase 5 - Análise e Avaliação de Riscos - Residual

Entende-se por risco residual a análise e avaliação dos riscos considerando os controles já existentes. Esse conceito permite que os controles sejam avaliados e posteriormente que sua efetividade seja comprovada durante os testes de auditoria.

1. Walkthrough - Avaliação dos Controles Existentes

Com o objetivo de confirmar a eficácia dos controles identificados nos processos ou áreas em estudo, é necessário realizar o walkthrough. No final dessa etapa, a informação disponível permitirá ao gestor responsável o conhecimento do processo ou área, e a eficácia, ineficácia ou inexistência dos controles para que seja construída uma análise de riscos residuais.

Para auxiliar na elaboração do Walkthrough deve-se utilizar as seguintes questões para análise:

- **Tipo?** Escrever o tipo de controle, ou seja, manual ou automático (sistema).
- **Controle?** Descrever o nome do controle. Controle é uma ação tomada para certificar-se de que algo se cumpra. Os controles também são meios usados para verificar que certa ação é eficiente ao seu propósito.
- **Descritivo do controle?** Conceituar / descrever o controle.
- **Objetivo do controle?** Escrever o objetivo do controle. Os controles e os meios devem ser dirigidos para um objetivo a ser atingido. Decidir qual o objetivo é o primeiro passo em qualquer processo de controle.
- **Qual o risco o controle está associado/mitigado?**
- **Periodicidade?** Escrever a periodicidade do uso do controle, ou seja, diário, quinzenal, mensal, etc.
- **Categoria?** Escrever a categoria do controle, ou seja, o preventivo, detectivo ou corretivo.
  - **Preventivo** - Desenhado para prevenir resultados indesejados. Reduzem a possibilidade de sua ocorrência e detecção.
  - **Detectivo** - Desenhado para detectar fatos indesejáveis. Detectam a manifestação/ocorrência de um fato.
  - **Corretivo** - Desenhado para corrigir os efeitos de um fato indesejável. Corrigem as causas do risco que seja detectado.
- **Resultado do *Walkthrough*?** Escrever o resultado dos procedimentos efetuados no *walkthrough* dos controles aplicados.
- **Parecer?** Escrever o parecer do controle analisado, ou seja, eficaz ou ineficaz.
- **Conclusão do *walkthrough*?** Tendo em vista a avaliação dos controles, escrever a conclusão geral sobre o *Walkthrough*.

Exemplo Processo:

Figura 41 - Avaliação de Controles

Nº	Riscos	Fator de riscos	Controle	Tipo	Descritivo do Controle	Objetivo de Controle	Periodicidade	Categoria	Resultado de Walkthrough	Parecer
1	Concessão de desconto indevido	Conluio entre gerente regional e gerente da loja	Não possui	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável
1	Concessão de desconto indevido	Ausência de bloqueio sistêma para cliente com restrição de crédito	Análise de crédito do cliente	Manual	Análise de crédito do cliente realizada pelo departamento administrativo da loja no momento da venda	Restríngir a venda para clientes que não estejam em conformidade de pagamento com a loja	Diário	Preventivo	Foi verificado que a análise do cliente é reliazada manualmente pela assistente e não existe nenhum bloqueio sistêmico que permita bloquear um cliente que esteja com dívida com a loja	Ineficaz
1	Concessão de desconto indevido	Ausência de análise de concessão de descontos	Senha individual para aplicação de desconto	Automático	Para descontos especiais ou acima da tabela, o gerente da loja deve inserir uma senha individual para a concessão do desconto	Garantir que apenas funcionarios cadastrados no sistema e com alçada de liberação, concedam desconto especiais para clientes	Diário	Preventivo	Foi verificado que o sistema não permite que um vendedor conceda descontos sem a autorização do gerente através de uma senha individual, bloqueando o desconto e alertando o gerente por e-mail quado existe uma tentativa indevida de concessão de desconto	Eficaz
1	Concessão de desconto indevido	Ausência de análise de concessão de descontos	Senha e contrassenha do gerente regional para desconto	Automático	Para liberações acima da alçada do gerente é necessária a aprovação do gerente regional. Uma senha é gerada automaticamente pelo sistema e é enviada para o gerente da loja, o desconto só é concedido caso o gerente regional envie uma outra senha	Não permitir a liberação de desconto acima das margens determinadas para os gerentes, sendo necessária a intervenção do gerente regional para casos especificos	Diário	Preventivo	Foi verificado que o sistema não permite que o gerente da loja conceda descontos sem a autorização de gerente regional. A autorização é realizada através de uma contrassenha encaminhada via aplicativo e a senha pode ser utilizada apenas uma vez	Eficaz
Conclusão sobre Walkthrough										
Baseado nos procedimentos executados acima, a processo de " vendas de serviços/produtos", está funcionando de acordo com o fluxograma levantado, sendo que foram identificados 5 controles para o processo. Três se mostraram eficazes para previnir os riscos. Cabe ressaltar que nossas verificações foram conduzidas de maneira amostral.										
Walkthrough - Controles Avaliados										
Qualidade de controles avaliados		Preventivos		Detectivos			Eficaz		Ineficaz	
5		5		0			3		2	

Walkthrough Processo

Fonte: Brasiliano (2016, p. 209).

2. Probabilidade x Impacto

Para realizar análise de riscos residuais (probabilidade x impacto) deve-se utilizar a metodologia e os critérios abordados no capítulo anterior Determinação do Nível de Probabilidade e Nível de Impacto. Abaixo quadro comparativo entre a análise de riscos inerentes x análise de riscos residuais. Exemplo Processo:

Figura 42 - Análise de Riscos Residuais

N °	Macroprocesso	Processo	Riscos	Porbabilidade						Relevância de impacto						
				Frequência / Exposição	Segurança	Intervalo	Nota X Peso	Média ponderada do impaco	Nível de probabilidade	Imagem	Financeiro	Legislação	Operacional	Nota X Peso	Média ponderada do impacto	Nível do impacto
				4	5	3	12			4	3	2	2	11		
1	Vendas	Vendas de produto	Concessão de desconto indevida	3	5	5	52,00	4,33	Muito Alta	3	4	1	3	32,00	2,91	Moderado
2	Vendas	Vendas de produto	Venda sem estoque fisíco	3	5	5	52,00	4,33	Muito Alta	4	4	2	4	40,00	3,64	Severo
3	Vendas	Vendas de produto	Fovorecimento de clientes	4	5	5	56,00	4,67	Elevada	3	4	1	3	32,00	2,91	Moderado
4	Vendas	Vendas de produto	Análise financeira equivocada	2	5	5	48,00	4,00	Muito Alta	3	3	2	5	35,00	2,18	Moderado
5	Vendas	Vendas de produto	Não ser cumprido o prazo de entrega de mercadoria para o cliente	4	5	5	56,00	4,67	Elevada	4	3	3	5	41,00	3,73	Severo

N °	Macroprocesso	Processo	Riscos	Porbabilidade						Relevância de impacto						
				Frequência / Exposição	Segurança	Intervalo	Nota X Peso	Média ponderada do impaco	Nível de probabilidade	Imagem	Financeiro	Legislação	Operacional	Nota X Peso	Média ponderada do impacto	Nível do impacto
				4	5	3	12			4	3	2	2	11		
1	Vendas	Vendas de produto	Concessão de desconto indevida	3	2	5	15,00	3,00	Alta	2	4	1	3	28,00	2,55	Moderado
2	Vendas	Vendas de produto	Venda sem estoque fisíco	4	5	5	21,00	4,20	Muito Alta	4	3	2	4	37,00	3,35	Moderado
3	Vendas	Vendas de produto	Fovorecimento de clientes	5	3	5	21,00	4,20	Muito Alta	2	3	1	3	25,00	2,27	Leve
4	Vendas	Vendas de produto	Análise financeira equivocada	3	3	5	17,00	3,40	Alta	2	4	2	4	32,00	2,91	Moderado
5	Vendas	Vendas de produto	Não ser cumprido o prazo de entrega de mercadoria para o cliente	4	3	5	19,00	3,80	Muito Alta	4	3	3	4	39,00	3,55	Severo

Análise de Risco Residual - Processo

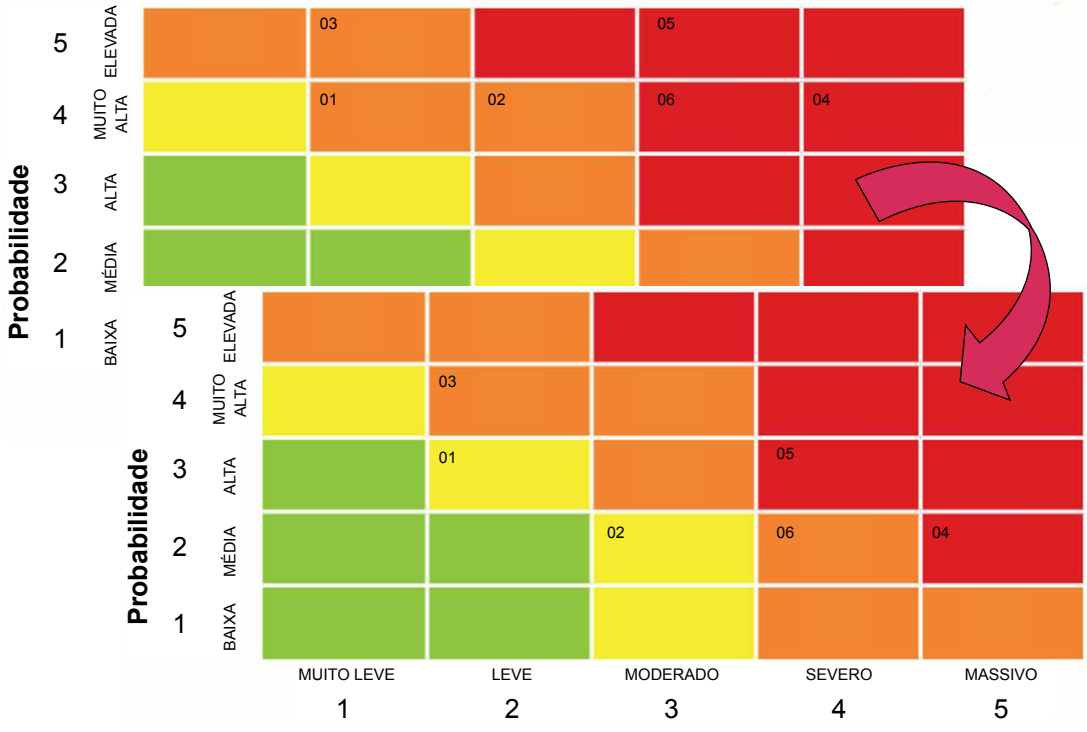
Fonte: Brasiliano (2016, p. 211).

3. Matriz de Riscos

Para elaborar a Matriz de Riscos Residuais utilizar a metodologia e os critérios do capitulo anterior Matriz de Riscos.

Abaixo quadro comparativo entre a matriz de riscos inerente x matriz de riscos residuais. Exemplo:

Figura 43 - Análise de Riscos Inerentes



Matriz de Risco Inerente

Fonte: Brasiliano (2016, p. 212).

4. Nível de Riscos

Para elaborar o Nível de Riscos Residuais utilizar a metodologia e os critérios estabelecidos no capítulo anterior Nível de Risco. A seguir, veja o quadro comparativo entre o nível de riscos inerentes x nível de riscos residuais.

Exemplo Processo:

Figura 44 - Nível de Riscos Inerentes

Riscos	Probabilidade	Impactos
Concessão de descontos indevido	4,2	2,55
Venda sem estoque fisíco	4,6	3,36
Favorecimento de cliente	5	2,27
Análise financeira equivocada	4,2	2,91
Não ser cumprido o periodo de entrega de mercadoria para o cliente	4,6	3,55
Total	22,60	14,64
Média	4,52	2,93
Nível de riscos		13,23

Nível de Riscos		
1 a 5	1	Verde
5,01 a 10	2	Amarelo
10,01 a 15	3	Laranja
15,01 a 25	4	Vermelho

Riscos	Probabilidade	Impactos
Concessão de descontos indevido	3	2,56
Venda sem estoque fisíco	4,2	3,36
Favorecimento de cliente	4,2	2,27
Análise financeira equivocada	3,4	2,91
Não ser cumprido o periodo de entrega de mercadoria para o cliente	3,8	3,55
Total	18,80	14,64
Média	3,72	2,93
Nível de riscos		10,69

Nível de Riscos		
1 a 5	1	Verde
5,01 a 10	2	Amarelo
10,01 a 15	3	Laranja
15,01 a 25	4	Vermelho

Nível de Risco Inerente - Processo

Fonte: Brasiliano (2016, p. 214).

f) Fase 6 - Respostas aos Riscos

É importante que exista a conscientização e comprometimento com o gerenciamento de riscos por parte da alta administração da empresa. Nesse contexto, os tomadores de decisão são os responsáveis por esse gerenciamento, ou seja, mediante a matriz de riscos deve-se identificar qual a resposta a ser adotada para tratamento do risco. Abaixo as estratégias que podem ser adotadas para o tratamento dos riscos:

- **Evitar o Risco:** Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Necessário preencher o formulário padrão de Risco Assumido.
- **Aceitar o Risco:** Neste caso, apresentam-se três alternativas: reter, reduzir ou transferir/compartilhar o risco.
- **Reter:** Manter o risco no nível atual de impacto e probabilidade. Necessário preencher o formulário padrão de Risco Assumido.
- **Reduzir:** Ações são tomadas para minimizar a probabilidade e/ou o impacto do risco.
- **Transferir e/ou Compartilhar:** Atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco.

O risco é assumido quando um tomador de decisão decide assumir riscos no quadrante vermelho ou laranja da Matriz de Riscos Residuais, tendo em vista a relação custo benefício ou por questões estratégicas. Este tipo de decisão vai contra a boas práticas de mercado. Sempre que um tomador de decisão resolver assumir riscos deve fazê-lo de maneira documentada para mantendo assim um registro, possibilitando que o mesmo seja acionado caso o risco assumido venha a se concretizar.

1. Planos de Ação

Depois de identificados, avaliados e mensurados, deve-se definir qual tratamento deve ser atribuído aos riscos. A priorização deve estar embasada na Matriz de Riscos Residuais, Diagrama de Causa e Efeito e Matriz SWOT. Os riscos localizados nos quadrantes vermelhos e laranjas devem receber prioridade no tratamento. Para elaboração do plano de ação é utilizada a técnica das perguntas 5W e 2H.

- **What? (O que?):** Medida em relação à causa prioritária;
- **Who? (Quem?):** Nome do responsável pela implementação da ação;
- **When? (Quando?):** Data limite para implementação da ação;

- **Where? (Onde?):** Onde a ação será implementada;
- **Why? (Por quê?):** Qual o motivo para realização da ação;
- **How? (Como?):** Descrever como será executada ação proposta;
- **How Much? (Quanto Custa?):** Qual o valor do investimento.

Exemplo:

Figura 45 - Análise de Riscos Inerentes

O que ocasiona o risco?	Criticidade	Controle	O controle é eficaz?	Quem faz parte nesse processo?	O que pode ser implementado?	Como deve ser realizado para melhoria?	Quanto custa?	Status
1- Furto de pertencentes pessoais								
Qualidade de imagem ruim	- 6	CFTV de segurança	Ineficaz	Gerência de segurança	Controle	Sustituição das câmeras de monitoramento por itens de melhor qualidade	R$ 50.000.00	Não realizado
2 - Roubo de carga								
Falta de treinamento do operador de CFTV	- 9	Central de segurança	Ineficaz	Gerência de segurança e recursos humanos	Controle	Aplicar treinametos específicos para todos os operadores de central de segurança	HH interno	Está em execução
3 - Sabotagem na cabine primária								
Ausência de CFTV em locais estratégicos	- 9	Alarme	Eficaz	Gerência de segurança	Teste	Aplicar teste de intrusão a cada seis meses no local	HH interno	Realizado
		Sensor de presença	Eficaz	Gerência de segurança	Teste	Aplicar teste de intrusão a cada seis meses no local	HH interno	Realizado
Falha na utilização do botão de pâmico	- 6	Botão de pânico	Ineficaz	Gerência de segurança empresa de monitoramento externo	Controle	Efetuar a revisão dos procedimentos de pronta respostas e alarmes do botão pânico realizado a adequação dos níveis de serviço	HH interno	Não Realizado

Plano de Ação

Fonte: Brasiliano (2016, p. 222).

2. Projeção Futura – Probabilidade x Impacto

Para que possam realizar uma Matriz de Riscos com projeção futura é necessário reavaliarmos a Análise de Riscos, partindo da premissa que o plano de ação previsto está ou será implementando.

Essa reavaliação é obtida na revisão dos fatores de riscos do diagrama de causa e efeito de cada risco, ou seja, tudo que foi tratado / implementado causará uma redução da probabilidade na matriz de riscos.

Exemplo:

Figura 46 – Comparativo Probabilidade x Impacto

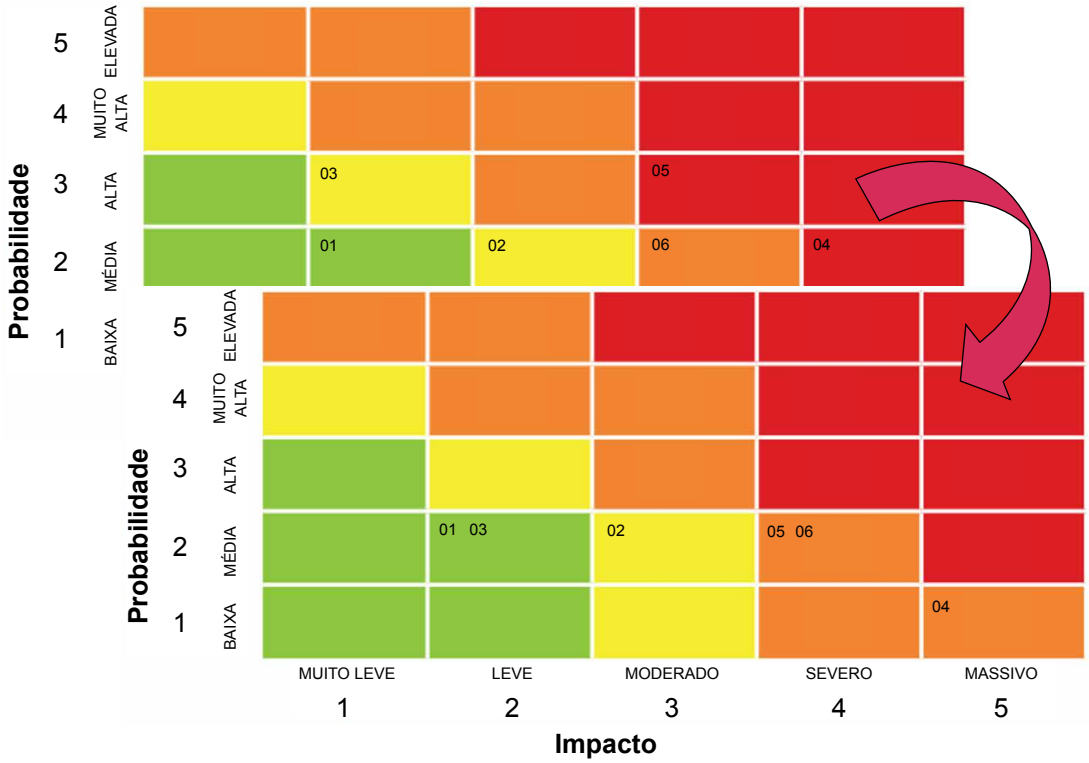
N º	Processo	Riscos	Porbabilidade						Relevância de impacto						
			Frequência / Exposição	Segurança	Intervalo	Nota X Peso	Média ponderada da probablidade	Nível de probabilidade	Imagem	Financeiro	Legislação	Operacional	Nota X Peso	Média ponderada do impacto	Nível do impacto
			4	5	3	12			4	3	2	2	11		
1	Segurança	Vandalismo	3	3	3	27,00	3,00	Alta	3	2	1	3	28,00	2,38	Leve
2	Segurança	Furto de veículos	2	2	2	20,00	2,22	Média	2	2	2	4	33,00	3,00	Moderado
3	Segurança	Furto de pertences pessoais	2	3	5	38,00	4,22	Muito Alta	2	2	1	4	24,00	2,18	Leve
4	Segurança	Sabotagem na cabine primária	4	2	3	22,00	2,44	Média	5	5	3	5	51,00	4,64	Massivo
5	Segurança	Desvio de mercadoria	4	3	3	30,00	3,33	Alta	3	5	2	4	39,00	3,50	Severo
6	Segurança	Roubo de carga	2	3	2	20,00	2,22	Média	3	5	4	4	43,00	3,91	Severo

N º	Processo	Riscos	Porbabilidade						Relevância de impacto						
			Frequência / Exposição	Segurança	Intervalo	Nota X Peso	Média ponderada da probablidade	Nível de probabilidade	Imagem	Financeiro	Legislação	Operacional	Nota X Peso	Média ponderada do impacto	Nível do impacto
			4	5	3	12			4	3	2	2	11		
1	Segurança	Vandalismo	3	2	2	21,00	2,33	Média	3	2	1	3	28,00	2,38	Leve
2	Segurança	Furto de veículos	2	1	2	15,00	1,78	Média	3	3	2	4	33,00	3,00	Moderado
3	Segurança	Furto de pertences pessoais	4	1	2	22,00	2,44	Média	3	3	2	4	24,00	2,18	Leve
4	Segurança	Sabotagem na cabine primária	2	1	1	12,00	1,33	Baixa	5	5	3	5	51,00	4,64	Massivo
5	Segurança	Desvio de mercadoria	4	1	2	22,00	2,44	Média	3	5	2	4	39,00	3,55	Severo
6	Segurança	Roubo de carga	2	2	1	14,00	1,56	Média	3	5	4	4	43,00	3,91	Severo

Fonte: Brasiliano (2016, p. 230).

Figura 47 - Comparativo Matriz de Risco

Risco Residual x Projeção Futura



Fonte: Brasiliano (2016, p. 231).

Figura 48 - Comparativo Nível de Risco

Risco Residual x Projeção Futura

Riscos	Probabilidade	Impacto
Vandalismo	3	2,36
Furto de veículos	2,42	3
Furto de pertences pessoais	3,83	2,18
Sabotagem na cabine primária	2,25	4,64
Desvio de mercadoria	3,33	3,55
Roubo de carga	2,42	3,91
Total	17,25	19,64
Média	2,88	3,27
Nível de riscos		9,41
Nível de Riscos		
1 a 5	1	Verde
5,01 a 10	2	Amarelo
10,01 a 15	3	Laranja
15,01 a 25	4	Vermelho

Riscos	Probabilidade	Impacto
Vandalismo	2,33	2,36
Furto de veículos	1,58	3
Furto de pertences pessoais	2,25	2,18
Sabotagem na cabine primária	1,33	4,64
Desvio de mercadoria	2,25	3,55
Roubo de carga	1,75	3,91
Total	11,49	19,64
Média	1,92	3,27
Nível de riscos		6,27
Nível de Riscos		
1 a 5	1	Verde
5,01 a 10	2	Amarelo
10,01 a 15	3	Laranja
15,01 a 25	4	Vermelho

Fonte: Brasiliano (2016, p. 232).

g) Fase 7 - Monitoramento e Análise Crítica

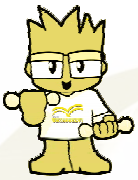
O monitoramento e a análise crítica devem ser planejados como parte do processo da avaliação de riscos e deve envolver a checagem ou vigilância de maneira regular. Podem ser periódicos ou acontecer em resposta a um fato específico. Devem ser monitorados:

- Plano de Ação;
- Grau de Risco - Matriz de Risco;
- Nível de Risco.

De forma clara e objetiva o monitoramento envolve dois processos:

- O primeiro é a verificação se o Plano de Ação proposto está sendo executado. Para isso devemos utilizar um farol, com os indicadores de Executado, em execução e não executado. Também devem ser acompanhados os resultados das ações e medidas propostas. Devem ser acompanhadas para saber se seus objetivos foram atingidos e se não foram quais as dificuldades encontradas e as ações corretivas.
- O segundo processo de monitoração diz respeito à evolução das condições dos riscos identificados e analisados. Neste caso deve-se montar um processo de acompanhamento se as condições listadas no diagrama de causa e efeito sofrem mudanças e ou alterações do ambiente. Este processo de monitoramento é de suma importância e deve ser acompanhado diretamente pelo gestor de riscos.

O monitoramento do plano de ação deve ser realizado mensalmente pelos facilitadores e responsáveis das áreas. O gestor deverá elaborar indicadores nos processos considerados críticos e nos processos com nível de riscos 3 e 4.



Atividades De Estudos:

1) A aplicação de técnicas e ferramentas de análise de riscos estão listadas na norma:

a) ISO 31000.
b) ISO 31004.
c) ISO 31010.
d) ISO 27005.

2) O método Brasiliano de Análise de Riscos possui, para a identificação dos processos críticos, a ferramenta BIA – Business Impact Analysis. Essa ferramenta possui dois critérios que devem ser analisados:

a) Probabilidade e Impacto.
b) Impacto no negócio e Tempo de tolerância.
c) Magnitude e Importância.
d) Tempo de tolerância e Magnitude.

3) Qual é o objetivo de utilizar a ferramenta do BIA – Business Impact Analysis no processo de gestão de riscos?

a) Saber a criticidade de riscos do processo e ou área.
b) Saber a criticidade para o negócio do processo e ou área.
c) Saber a importância de utilização operacional do processo e ou área.
d) Todas as alternativas acima estão corretas.

4) Qual é o objetivo de utilizar a ferramenta Diagrama de Causa e Efeito no processo de gestão de riscos?

a) Identificar a motricidade dos riscos identificados.
b) Identificar a importância dos fatores de riscos.
c) Identificar as causas/fatores de risco de cada risco identificado.
d) Todas as alternativas acima estão erradas.

5) Qual é o objetivo de utilizar a ferramenta Matriz SWOT no processo de gestão de riscos?

a) Identificar a relevância dos fatores de riscos, ressaltando os mais motrizes.
b) Identificar os fatores de riscos com mais frequência.
c) Identificar os fatores de riscos de cada risco.
d) Todas as alternativas acima estão corretas.

6) No Método Brasiliano de Análise de Riscos, a probabilidade é analisada sob três critérios:

a) Segurança/Controle, Frequência/Exposição e Intervalo.
b) Imagem, Frequência/Exposição e Intervalo.
c) Segurança/Controle, Intervalo e Operacional.
d) Vulnerabilidade, Frequência/Exposição e Segurança/Controle.

7) O que difere o risco inerente do residual é:

a) A avaliação de riscos é feita levando em consideração os controles existentes.
b) A avaliação de riscos é feita levando em consideração os controles a serem implantados.
c) A avaliação de riscos é feita sem levar em consideração os controles existentes.
d) Todas as alternativas acima estão corretas.

8) A eficácia dos controles pode ser medida observando-se:

a) A diminuição da criticidade do risco residual frente ao risco inerente.
b) A diminuição da criticidade somente do risco inerente.
c) A diminuição da criticidade do risco residual com a futura implantação de controles.
d) As alternativas b e c estão corretas.

9) O processo de monitoramento e análise crítica deve ter foco:

a) Nas condições do risco e na implantação do plano de ação.
b) Nas condições do risco, implantação do plano de ação e das variáveis externas.
c) Somente na condição do risco.
d) Somente na implantação do plano de ação.

IBGC. Cadernos de Governança Corporativa. **Gerenciamento de Riscos Corporativos** - Evolução em Governança e Estratégia, 2017 - Caderno nº 19 Publicado em Maio de 2017.

ARAÚJO, Marcus Augusto Vasconcelos. **Percepção e Comportamento de riscos nas organizações**. São Paulo: Sicurezza, 2013.

RASILIANO, Antonio Celso Ribeiro Brasiliano. **Gestão de Continuidade de Negócios**. São Paulo: Sicurezza, 2013.

BRASILIANO, Antonio Celso Ribeiro Brasiliano. **Gestão de Riscos de Fraude**: Abordagem Preventiva – Fraud Risk Assessment - FRA. São Paulo: Sicurezza, 2015.

MACIEIRA, André. **Gestão de Riscos Positivos**. São Paulo: Sicurezza, 2011.

ORIÁ FILHO, Humberto Ferreira. **As Fraudes Contra as Organizações e o Papel da Auditoria Interna**. São Paulo: Editora Sicurezza, 2011.

Algumas Considerações

O processo de Gestão de Riscos Corporativos, Método Brasiliano - Avançado, possui o *Framework* adaptado da ISO 31000, porém todo o seu conteúdo, o como fazer com métricas e ferramentas, possui os fundamentos integrados do COSO I e II e da ISO 31000, utilizando ferramentas e técnicas da ISO 31010.

Esse processo facilita uma análise e avaliação de riscos estruturada, onde é possível identificar riscos, fatores e controles e através de métricas mensurar a probabilidade e o impacto do risco, inerente ou residual, ajudando você a priorizar recursos e oferecendo uma visão estratégica para a alta direção.

Para finalizar o livro, vamos conferir uma breve revisão de tudo o que foi estudado.

Os riscos estratégicos, operacionais, financeiros, legais e externos que afetam as empresas globais e que são potencialmente prejudiciais para as organizações brasileiras requerem, o fortalecimento de práticas inerentes à sua governança corporativa. Com base na forte dinamicidade do ambiente do mercado, mundo VUCA, podemos sugerir os seguintes passos para que as empresas tenham processos estruturados de gestão de riscos e, desta forma possam trabalhar de forma preventiva:

1. **Gerenciar a motricidade dos fatores de riscos:** A empresa precisa adotar uma gestão integrada de riscos para identificar e administrar as correlações entre todos os fatores de riscos, através da Matriz SWOT, visando saber onde colocar controles;

2. **Alimentar uma forte cultura de controles com o processo descentralizado**: A administração da empresa tem que criar uma cultura que enfatize a importância do dono do processo ser o dono do risco, com isso a ética, deve ser enfatizada integrada com o gerenciamento de riscos. Incentivos de remuneração devem ser alinhados com a criação de valores em longo prazo e com a proteção à marca;

3. **Fornecer informações em "tempo real"**: A empresa precisa implantar sistemas de informações internos e mecanismos de comunicação para assegurar que a Diretoria Executiva e o Conselho de Administração recebam informações corretas, em tempo real, sobre as causas e os impactos, não só financeiros, mas também legais, operacionais e ligados a reputação, bem como as possíveis soluções para os problemas;

4. **Enfrentar os riscos com baixa frequência e alto impacto**: A empresa deve empregar "testes de estresse" para assegurar que os controles internos e os planos para a continuidade dos negócios poderiam resistir a um evento de alto impacto ou, pelo menos, que pudessem dar flexibilidade para responder rapidamente a cenários adversos.

O importante é que todas as empresas, independentemente do perfil e do porte, precisam conhecer a efetiva dimensão dos riscos das suas atividades em que estão envolvidas. Mesmo não podendo evitar os riscos, as empresas podem melhorar seu controle sobre o ambiente, prevenindo, amenizando ou recuperando-se mais rapidamente desses eventos. Dessa forma terão condições de sobreviverem com maior agilidade e flexibilidade.

O Método aqui descrito - Método Brasiliano de Gestão e Análise de Riscos - é uma técnica para auxiliar o gestor na priorização do tratamento dos riscos, possibilitando integrar as origens de cada risco com seu nível de influência para sua concretização e de resposta aos riscos. Auxilia de forma direta na construção da matriz de riscos e a matriz de priorização de ações.

Esperamos que com esta técnica possamos facilitar a tomada de decisão dos responsáveis pela gestão de riscos e auxiliar a implantação de medidas reais preventivas e contingenciais.

Referências

ABNT NBR ISO 31.000:2009 - **Gestão de Riscos** - Princípios e Diretrizes.

ABNT NBR ISO 31010:2009, **Gestão de Riscos** - Técnicas para o processo de avaliação de riscos.

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em Riscos**: Gestão Integrada em Corporativos. São Paulo: Editora Sicurezza, 2016.

COSO 2013 - **Committee of Sponsoring Organizations of the Treadway Commission** - Internal Control - Integrate Framework.

COSO ERM - **Committee of Sponsoring Organizations of the Treadway Commission** - Enterprise Risk Management.