METODOLOGIA DE AVALIAÇÃO DOS RISCOS OPERACIONAIS

Vitória, 23 de agosto de 2018

Sumário

1. Conceito:

Termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender "risco" como possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação da incerteza, desta forma, o IBGC trouxe a definição de risco descrita por Faber, Manstetten e Proops, 1996 que o define como:

> Evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência. Incerteza: evento futuro identificado, ao qual não é possível associar uma probabilidade de ocorrência. Ignorância: eventos futuros que, no momento da análise, não poderão sequer ser identificados, muito menos quantificados (exemplo: eventos decorrentes de sistemas complexos como o climático – as consequências do aquecimento global são imprevisíveis).

Definições estas que se assemelham a Resolução nº 4.557, de 23/02/2017 do Banco Central do Brasil (BCB) que define Risco Operacional como possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas.

2. Eventos de Riscos

O artigo 32 da Resolução nº 4.557 do BCB define em seu § 2º, oito eventos de riscos que podem ser consideradas as portas de entrada destes para a companhia:

I. Fraudes internas;
II. Fraudes externas;
III. Demandas trabalhistas e segurança deficiente do local de trabalho;
IV. Práticas inadequadas relativas a clientes, produtos e serviços;
V. Danos a ativos físicos próprios ou em uso pela instituição;
VI. Situações que acarretem a interrupção das atividades da instituição;
VII. Falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI);
VIII. Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição.

3. Origem dos eventos

Os eventos de risco podem surgir tanto de fatores externos quanto internos e possuir natureza estratégica, operacional ou financeira. Podem ser riscos que se encontram inerentes na operação ou até mesmo riscos estratégicos para atingimento de determinados objetivos. Resta para a área de GRC avaliar se ao assumir estes riscos a companhia possui a salvaguarda para casos de ocorrência, inclusive provisionando valores de possíveis sanções punitivas, e/ou perdas no processo.

4. Processo de Avaliação dos Riscos:

Utilizando definições da ISO 31.000/2018, o processo de avaliação dos Riscos Operacionais é feito através de três fases que visam a otimização e controle das operações.

Para análise e gestão dos riscos, serão utilizadas metodologias adotadas pela Instituto Brasileiro de Governança Corporativa (IBGC), as diretrizes dadas pela Resolução nº 4.557, de 23/02/2017 do BCB, além dos dispostos da ISO 31.000/2018. Ressaltamos que o processo de avaliação de riscos é um subprocesso da Gestão de Riscos sendo a parte de

responsabilidade da área de GRC, os demais pilares de Risco são tratados diretamente pela alta administração da companhia.

4.1. Identificação do risco

Trata-se da definição do conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização. A identificação é realizada por análise e mapeamento das possíveis causas advindas dos eventos de riscos descritos na Resolução nº 4.557, de 23/02/2017 do BCB.

Para identificar um risco, são realizadas uma série de questionamentos entre os membros da área de GRC para definir se em determinado processo há ou não indicativos de riscos, para tal, foram utilizadas questões definidas pela ISO 31.000/2018 que traz os seguintes tópicos para identificação:

- Fontes tangíveis e intangíveis de risco;
- Causas e eventos;
- Ameaças e oportunidades;
- Vulnerabilidades e capacidades;
- Mudanças nos contextos externos e internos;
- Indicadores de riscos Emergentes;
- Natureza e valor dos ativos e recursos;
- Consequências e seus impactos nos objetivos;
- Limitações de conhecimento e confiabilidade nas informações;
- Fatores temporais;
- Vieses e hipóteses de crenças dos envolvidos.

Se ao menos um destes pontos for observado pela área de GRC no processo avaliado, existe um indicativo de risco ao qual deverá ser avaliado com maior riqueza de detalhes nas demais fases do processo.

4.2. Análise de Risco

Os riscos são avaliados através da medição de seu grau de exposição em matriz simples 4 x 4 por entender que este modelo seja o que melhor se adeque para a realidade da companhia, embora tenhamos analisados outros modelos, o estudo de Filipa Carvalho (2010) nos direcionou para o uso desta metodologia por ela não mostrar distorção dos demais modelos de mercado e por ser uma metodologia validada pelo IBGC e pela ISO 31.000/2018.

Para alcance da classificação de risco, são apuradas informações referentes a Probabilidade de ocorrência X Impacto, o cruzamento destas informações evidencia o grau de exposição do risco identificado.

4.2.1. Análise da Probabilidade

Para entendimento desta avaliação, definimos o conceito de probabilidade como o estudo das chances de ocorrência de cada risco identificado.

A régua de probabilidade de ocorrência em quatro níveis que vão do **Improvável** (nível esperado pela organização) ao **Mais que provável** (probabilidade crítica que deve ser mitigada). Não foram definidos percentuais para definição da probabilidade além da escala, pois seguimos os modelos usuais de mercado que não vem adotando esta metodologia devido à dificuldade em encontrar uma referência válida de definição uma vez que o peso de cada ocorrência se difere de um processo para o outro.

Figura 1: Escala Probabilidade

Probabilidade de ocorrência

	Classificação	Critério
4	Mais que provável	Acertiva de ocorrer o evento é muito frequente
3	Provável	Acertiva de ocorrer o evento é frequente
2	Possível	Acertiva de ocorrer o evento em algumas vezes
1	Improvável	Hipótese quase nula

Fonte: Autor

4.2.2. Análise do Impacto

Seguindo as definições usuais, para melhor entendimento de nossa avaliação, impacto será definido como efeito monetário positivo ou negativo surgido junto à eminência de risco. Em linhas gerais, impacto é quanto custa o risco.

A escala de impacto será no primeiro momento apurada de forma qualitativa, medindo o quão grave poderá ser a sua ocorrência em determinado risco com base nos critérios ilustrados na Figura 2. Sempre que na avaliação qualitativa o impacto se mostrar alto ou extremo, será realizada uma análise quantitativa para apurar os valores que o risco representa para a empresa e desta forma ilustrar de maneira fidedigna a realidade deste, em caso de impacto qualitativo moderado ou baixo, não serão realizadas maiores análises preliminarmente por se enquadrarem ao nível de impacto aceitável, salvo se a exposição do risco se mostrar alta.

A metodologia de quantificação dos riscos altos e extremos será definida com base em sua natureza, época e extensão. Serão realizados testes que transpareçam o impacto monetário que o risco poderá causar à companhia, às definições de cada avaliação serão evidenciadas pela área de GRC a fim de dar suporte ao estudo.

Figura 2: Escala de Impacto

	CLASSIFICAÇÃO	CRITÉRIO
4	EXTREMO	Inviabiliza o alcance dos objetivos da atividade, processos ou da linha de negócios; Representa descumprimento de leis ou regulamentações que comprometem fortemente a imagem da empresa; Fatalidade e/ou destruição dos meios, instalações ou equipamentos; Perda de vida humana.
3	ALTO	Impacta fortemente no alcance dos objetivos da atividade, processos e linha de negócios; Representa descumprimento de leis ou regulamentações que comprometem a imagem da empresa; Fraude independente do dano causado, de qualquer natureza; Dano a integridade fisica.
2	MODERADO	Dificulta a execução da atividade, processo e linha de negócio; Representa descumprimento de leis ou regulamentações que não comprometem a imagem da companhia; Culmina na insatisfação e/ou perda de clientes.
1	BAIXO	Poderá afetar a atividade e o processo, gerando um impacto referente a eficiência do mesmo com relação a custo e prazo; Pode apresentar um leve efeito efeito sobre o alcance do objetivo da linha de negócio

Fonte: Autor

5. Avaliação dos Riscos

Após definido o grau de impacto e de probabilidade de risco qualitativamente, as informações são cruzadas na Matriz simples 4x4 para se obter o grau de exposição de cada risco avaliado. A probabilidade de ocorrência é medida de 1 a 4 e o impacto segue a mesma linha de raciocínio, sendo 1 para o melhor dos cenários e 4 para o inaceitável na tratativa de riscos.

Cruzando as avaliações, obtemos uma escala de risco que varia entre 1 e 16, desta forma, o grau de exposição será determinado pelo surgimento de 4 quartis, classificando os riscos como:

- Baixo (1 – 4);
- Médio (5 – 8);
- Alto (9 – 12);
- Extremo (13 – 16).

Figura 3: Matriz de Avaliação

ER= I x P		IMPACTO			
		1	2	3	4
		BAIXO	MODERADO	ALTO	EXTREMO
PROBABILIDADE					
4	Mais que provável	4	8	12	16
3	Provável	3	6	9	12
2	Possível	2	4	6	8
1	Improvável	1	2	3	4

Fonte: O autor

O *Target da* companhia é que todos os riscos estejam no quartil 1 com a classificação de risco baixa, sendo assim, todos os riscos classificados como Médios, Altos e Extremos serão trabalhados para obter mitigação e que os riscos líquidos sejam considerados aceitáveis.

A definição de risco líquido será realizada pela seguinte equação:

ERL = (I –CI) x (P x CP)

Onde:

I = Impacto

P = Probabilidade

CI = Controle do Impacto

CP = Controle de Probabilidade

Definidos todos os parâmetros dos riscos de determinado processo e avaliado o grau de exposição ao qual este se encontra, serão realizadas análises qualitativas acerca dos impactos causados por este na companhia.

Para utilização de análise e avaliação quantitativa, são estabelecidos dois critérios chaves a fim de tratar apenas riscos que ao ver da instituição, são considerados **relevantes** para a operação. A fim de facilitar o entendimento, definimos como riscos relevantes aqueles que dificultam o andamento do processo e geram perdas significativas de caixa. Perdas significativas são as classificadas como de alto ou extremo na avaliação qualitativa de impactos.

Desta forma, os critérios definidos pela área de GRC para quantificar os riscos são:

- **Evidência de Riscos Significativos:** Quando a análise qualitativa de probabilidade apontar indícios de que o risco é considerado alto ou extremo, ele será automaticamente mensurado.
- **Exposição média ou superior:** Como o *Target* da companhia é que os riscos sejam baixos, sempre que a exposição do risco for considerada média, alta ou extrema, será realizada uma quantificação dos impactos.

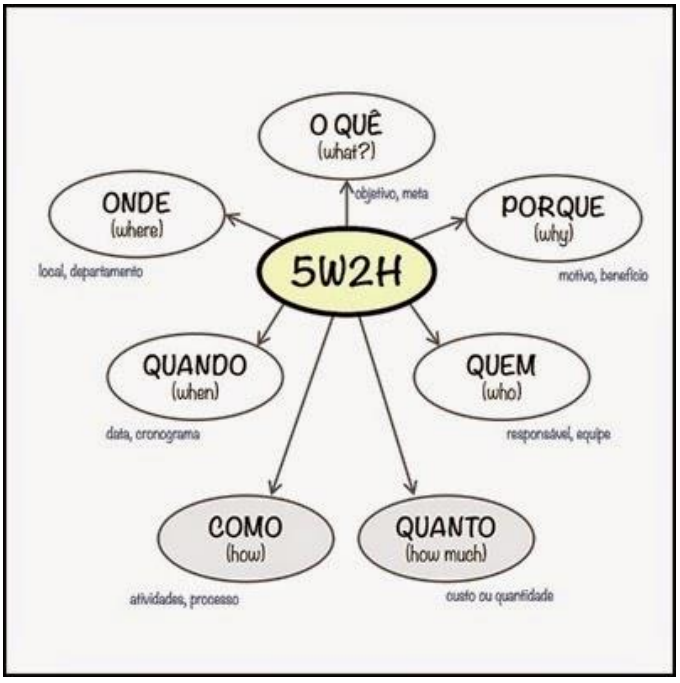
6. Tratamento dos Riscos

Definidos os riscos relevantes, a alta administração, o setor responsável pelo processo e a área de GRC definirão estratégias para tratar os riscos mapeados, sempre com a finalidade de atingir o objetivo geral da companhia e estabelecer um padrão de controle estruturado que garanta segurança razoável para o processo.

6.1. Definição de Planos de Ação (PA)

Optamos pela utilização do modelo 5W2H para definição dos Planos de Ação (PA) da área responsável pelo processo, com a finalidade de trazer a exposição do risco para o nível baixo, pertencente ao primeiro quartil de avaliação.

Figura 4: Metodologia 5W 2H



Fonte: Gustavo Periard

Todo Plano de Ação criado será acompanhado pela área de GRC da companhia, deste a fase de implantação dos planos quanto na validação futura de sua efetividade. Os papéis de

trabalho das avaliações serão anexados aos relatórios de risco e acompanhamento de Planos de Ação.

6.2. Controles

As análises e avaliações iniciais são acerca dos riscos considerados brutos, porém, em processos que já existam controles devidamente estruturados, estes serão avaliados juntamente como o processo em geral, desta forma o resultado do risco bruto já engloba a relevância do controle adotado.

Com base nesta avaliação, poderá ser obtido o nível de eficiência de cada controle empregado, logo, se o grau de exposição for considerado alto ou extremo, será a constatação de que o controle empregado no momento é ineficaz e precisará de uma avaliação mais apurada, que será desenvolvida através de Plano de Ação e será analisada ciclicamente.

Desta forma, sempre que for criado um PA para mitigar um risco relevante, serão criados controles e estes por sua vez deverão ser testados constantemente, seja pela área de GRC, seja pela Auditoria Interna, visando obter maior eficiência e menor risco em cada processo.

6.3. Provisionamento

Segundo CPC 25, provisão é um passivo de valor ou prazo incerto, ou seja, um risco cuja exposição é considerada alta ou extrema pode, por hermenêutica, ser considerado como uma provisão, uma vez que não é possível estipular um prazo para que ocorra, tampouco valores. Estes por sua vez estão mensurados através de estimativas, mas podem no melhor dos cenários nunca ocorrer.

Conforme estipulado no parágrafo 14 do CPC 25, uma provisão deve ser reconhecida quando:

(a) a entidade tem uma obrigação presente (legal ou não formalizada) como resultado de evento passado;

(b) seja provável que será necessária uma saída de recursos que incorporam benefícios econômicos para liquidar a obrigação; e

(c) possa ser feita uma estimativa confiável do valor da obrigação.

Conforme discorrido no tópico acerca da origem dos eventos, estes podem ser de natureza estratégica da companhia, ou até mesmo pode ocorrer de a área optar por assumir o risco identificado, assim acorrendo, será anexada a avaliação quantitativa do risco e sua exposição para a companhia junto do relatório do setor, e se, o impacto deste for superior a 0,5% do Patrimônio Referência da companhia, os valores deverão ser documentados e provisionados contabilmente para resguardar a empresa de quaisquer eventos futuros que podem vir a comprometer o funcionamento das atividades.

7. Sistemas de gerenciamento de risco

A companhia criou seu próprio sistema de gerenciamento de risco, onde serão cadastrados e armazenados todos os riscos identificados. O sistema conta com a metodologia da empresa e está devidamente parametrizado para definir o grau de risco com base em cada evento identificado, desta forma o grau de risco será evidenciado de acordo com pesos informados em cada evento e trazendo automaticamente a ponderação de probabilidade e impacto.

Como medida preventiva de vieses, o preenchimento das *questions* será realizada entre o setor responsável pelo risco e pela área de GRC, caso haja desentendimento em qualquer um dos temas abordados, será realizada consulta da alta administração e os dados lançados serão os definidos por decisão da diretoria.

7.1. Questionário de avaliação

O questionário de avaliação contém os pesos definidos para cada bloco de evento de risco, bem como o de cálculo de impacto destes. Cada peso foi definido em conjunto pela área de GRC e a alta administração da companhia de acordo com a realidade atual de empresa, desta forma, os pesos e as perguntas poderão ser alteradas ao longo do tempo, sempre que verificada chance de melhoria do processo.

7.1.1. Avaliação de Probabilidade

O questionário de avaliação de probabilidade conta com 48 perguntas com diferentes pesos e que serão cruciais para definição da probabilidade de ocorrência do risco identificado, porém, não serão respondidas 48 questões para cada risco, visto que cada bloco que questões é relacionado a um evento diferente, desta forma, ao selecionar os eventos referentes a cada risco na fase de Identificação das origens de risco, serão selecionas apenas os questionários relativos àquele risco.

7.1.2. Avaliação de impacto

Para mensurar o impacto de cada risco de maneira qualitativa, foram definidas 10 questões com diferentes pesos, diferente da análise de probabilidade, nesta etapa serão respondidas todas as questões e o impacto será definido com base no somatório geral de questões com base nos quartis previamente definidos.

Desta forma, poderá ser obtido com maior precisão o que o impacto de cada risco causará de maneira qualitativa ao processo e trará o indício de avaliação qualitativa para que sejam realizadas maiores avaliações nestes.e

7.2. Mensuração dos dados

A mensuração final do risco ocorrerá pelo somatório dos seguintes fatores:

- Cálculo da média ponderada das questões binárias com base no peso de cada questão;
- Aplicação da média ponderada dentro do quartil de risco definido pela metodologia.

Esta aplicação estatística ocorre para trazer mais segurança ao processo de avaliação do risco e blindar o processo quanto a interferências externas.

8. Monitoramento Contínuo

A área de GRC junto com a Auditoria Interna promoverão o monitoramento contínuo e avaliação dos riscos identificados buscando constantes melhorias e eficiência nos trabalhos.

Referências

BANCO CENTRAL DO BRASIL. Resolução nº 4.557 de 23 de fevereiro de 2017. **Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.** Brasília, 2017.

BRASILIANO, Antônio C. Ribeiro. **Método avançado de análise de risco: Resposta aos riscos Corporativos** – Método Brasiliano, 2009.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Estrutura Integrada: Sumário Executivo e Estrutura e Gerenciamento de Riscos na Empresa**.2007.

CPC. **Pronunciamento Técnico 25. Provisões, Passivos Contingentes e Ativos Contingentes**. Brasília, 2009.

FILIPA, Carvalho. AVALIAÇÃO DE RISCO: **Comparação entre vários métodos de avaliação de risco de natureza semi-quantitativa**. VI Encontro Nacional de Riscos, maio 2010.

Instituto Brasileiro de Governança Corporativa. **Guia de orientação para o gerenciamento de riscos corporativos / Instituto Brasileiro de Governança Corporativa**; coordenação: Eduarda La Rocque. São Paulo, SP: IBGC, 2007 (Série de Cadernos de Governança Corporativa, 3).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 31000: **Gestão de Risco,** 2018.