MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
CENTRO DE CONTROLE INTERNO DO EXÉRCITO
(CENTRO GENERAL SERZEDELLO CORRÊA)

NOTA TÉCNICA DE CONTROLE INTERNO Nr 01 – 11 de MAIO de 2016
GERENCIAMENTO DE RISCOS ÁREA ADM

1. INTRODUÇÃO

A utilização da metodologia de planejamento com base em riscos é uma prática moderna e adequada ao novo papel da auditoria, como uma ferramenta que agrega valor à gestão, e perfeitamente aplicável ao Comando do Exército.

Riscos são eventos negativos que podem impedir a criação de valor ou mesmo destruir o valor existente influenciando o atingimento dos objetivos de uma organização.

Antes de adentrar ao assunto é importante fazer a seguinte distinção, no que se refere à responsabilidade. As atribuições de identificação, análise, avaliação e manejo dos riscos é do Cmt/Ch/Dir de OM. O Controle Interno busca apresentar garantias de que tais riscos estão sendo gerenciados adequadamente por suas UG, auxiliando a organização a identificar e avaliar exposições significativas a riscos e contribuindo para a melhoria dos sistemas de gestão.

A fim de subsidiar o nível de atuação da Unidade de Controle Interno, particularmente no que se refere ao diagnóstico preliminar, há a necessidade de se identificar a maturidade da OM bem como a abordagem da auditoria interna a ser levada em consideração, sob a perspectiva do Controle Interno, no que se refere a riscos. Para tanto, é apresentada a tabela 1, fim de subsidiar este diagnóstico, com relação ao grau de maturidade de riscos.

Tabela 1. Grau de Maturidade de Riscos x Abordagem da Auditoria Interna

GRAU DE MATURIDADE DE RISCOS	CARACTERÍSTICAS PRINCIPAIS EVIDENCIADAS	ABORDAGEM DA AUDITORIA INTERNA
INGÊNUO	Nenhuma abordagem formal desenvolvida para a Gestão de Riscos.	Promove a Gestão de Riscos e se baseia na avaliação de riscos da própria auditoria.
CONSCIENTE	Abordagem da Gestão de Riscos dispersa em "silos".	Promove a abordagem corporativa para a gestão de riscos e se baseia na avaliação de riscos realizada pela própria auditoria.
DEFINIDO	Estratégia e políticas implementadas e comunicadas, apetite por riscos definido.	Facilita a Gestão de Riscos/Relaciona-se com a Gestão de Riscos, e usa a avaliação de riscos pela direção/gerência, conforme apropriado.
GERENCIADO	Abordagem corporativa para a Gestão de Riscos, desenvolvida e comunicada.	Audita os processos de Gestão de Riscos e utiliza a avaliação de riscos pela direção/gerência conforme apropriado.
HABILITADO	Gestão de Riscos e Controles Internos totalmente incorporados às operações.	Audita os processos de Gestão de Riscos e utiliza a avaliação de riscos pela direção/gerência conforme apropriado.

FONTE: De Cicco, 2007.

2. METODOLOGIA

O método pressupõe a construção de matrizes de risco para avaliação de probabilidades e impactos em relação às etapas de operacionalização de quaisquer processos de gestão, conforme descrito no Artigo "Metodologia de auditoria com foco em processo e risco", do Tribunal de Contas da União (BRASIL, 2015).

A metodologia proposta viabiliza a avaliação de riscos e controles e tem como referência o modelo ERM (*Enterprise Risk Management*), do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nas demonstrações contábeis das empresas.

O modelo considera que a gestão de riscos das instituições deve ser avaliada segundo oito componentes (dimensões) que lhe são intrínsecos (COSO, 2004). Nessa linha, a presente metodologia se propõe a avaliar os cinco elementos centrais do modelo, os quais podem ser traduzidos em perguntas que, didaticamente, facilitam o entendimento dos pontos:

a) fixação de objetivos: a unidade fixou objetivos para o processo ou para a política pública?

b) identificação de eventos: quais eventos podem representar risco aos objetivos do processo ou da política pública?

c) avaliação de riscos: qual é a significância dos riscos identificados em termos de probabilidade e impacto de ocorrência?

d) resposta a riscos: a organização implementou controles em resposta aos riscos identificados?

e) atividades de controle: qual é a qualidade dos controles internos estabelecidos e em que medida eles asseguram que os riscos relacionados sejam mitigados a um nível aceitável?

2.1 PROCEDIMENTOS

2.1.1 IDENTIFICAÇÃO E REGISTRO DE OBJETIVOS E PROCESSOS CRÍTICOS

Nesta fase, é preciso levantar e entender a legislação aplicável ao objeto, o regimento interno da organização, trabalhos anteriores de órgãos de controle interno e externo sobre o assunto, artigos acadêmicos ou técnicos, bem como outras informações disponíveis.

Deve-se, então, identificar os objetivos de cada atividade e/ou política pública a ser auditada, bem como compreender e registrar as etapas do processo de trabalho que compõem a atividade administrativa, desenvolvidas para alcançar os objetivos estabelecidos.

Como exemplo, no caso do processo de descentralização de recursos da União para outros entes públicos ou privados por meio de transferências voluntárias de recursos, poder-se-ia dividir o processo nas seguintes etapas: a) motivação da transferência; b) seleção do recebedor da descentralização; a) celebração do ajuste; b) acompanhamento da execução; e c) análise de prestação de contas.

2.1.2 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.

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 organização. Neste contexto, foi adaptado o diagrama de causa e efeito da qualidade para a área de Gestão de Riscos, conforme Macro Causas abaixo:

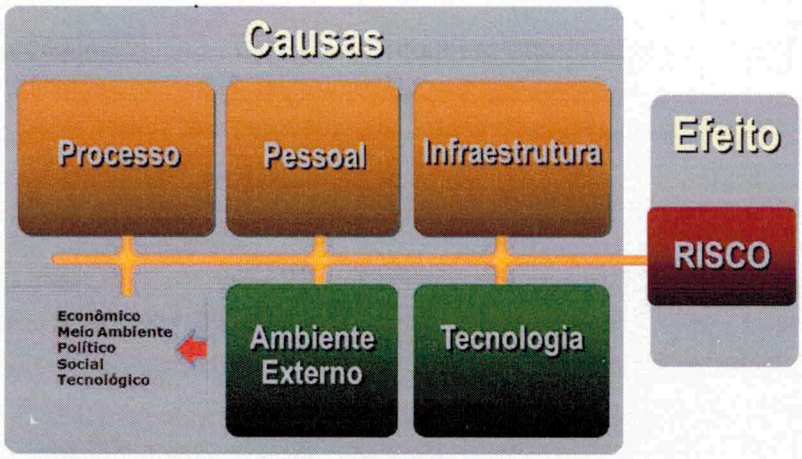

Figura 1 – Macro Causas

- **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 organização.
- **Tecnologia:** influência dos sistemas de informação utilizados pela organização 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 abaixo:

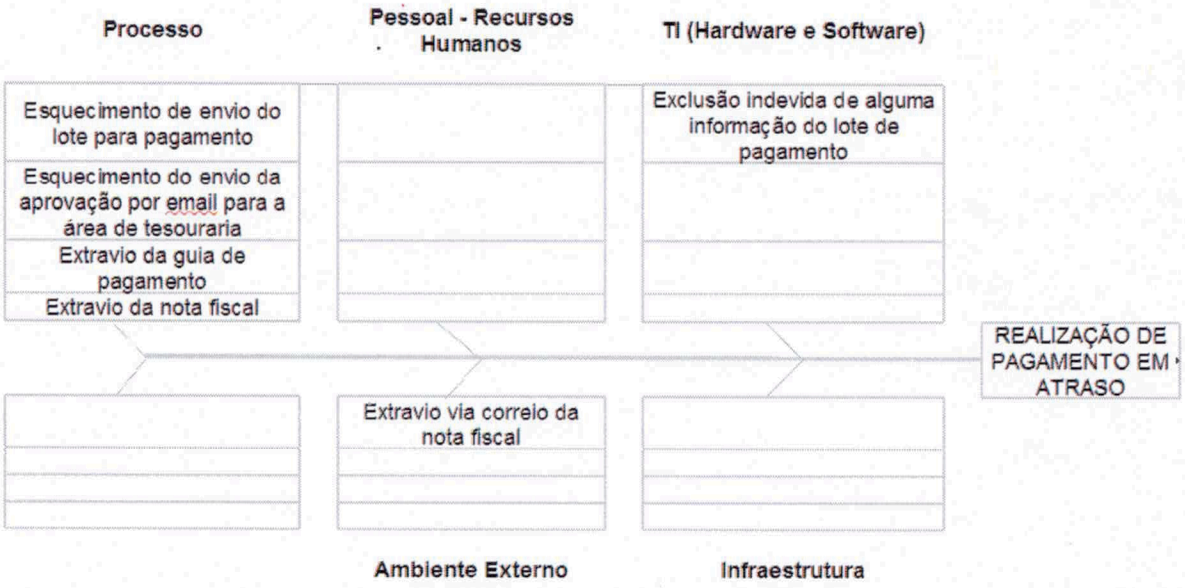

Figura 2 – Diagrama de Causa e Efeito

Ressalta-se 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.

2.1.3 ANÁLISE E AVALIAÇÃO DE RISCOS

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 de os riscos virem a acontecer e calcular seus respectivos impactos nos processos do Exército.

Os riscos são avaliados de maneira qualitativa (subjetiva), ou seja, utiliza critérios preestabelecidos com uma escala de valoração para a determinação do nível do risco. A metodologia a ser utilizada para a avaliação de riscos possui dois parâmetros claros a serem analisados:

a) saber qual a chance, a probabilidade, dos riscos virem a acontecer, frente à condição existente de cada processo e área de negócio do Exército; e

b) calcular o impacto caso ocorra o risco.

A análise qualitativa de risco empregada no diagnóstico tem por objetivo realizar uma análise subjetiva dos riscos percebidos na execução dos processos ou relacionados aos elementos que os influenciam (ambiente, recursos, etc.).

Os termos relacionados à probabilidade de risco e impacto do risco foram descritos em termos qualitativos como: elevado, muito alto, alto, médio e baixo, aos quais foram atribuídos os seguintes valores, respectivamente: 5, 4, 3, 2, e 1.

A qualificação das probabilidades e impactos é descrita abaixo:

Tabela 2. Probabilidades e impactos

CLASSIFICAÇÃO	PROBABILIDADE	IMPACTO
Elevada(o)	O evento de risco tem elevada probabilidade de ocorrer.	Se o evento de risco ocorrer, impacta outros processos muito fortemente.
Muito Alta(o)	O evento de risco tem altíssima probabilidade de ocorrer.	Se o evento de risco ocorrer, impacta outros processos de forma direta.
Alta(o)	O evento de risco tem alta probabilidade de ocorrer.	Se o evento de risco ocorrer, não impacta outros processos.
Média(o)	O evento de risco tem probabilidade média de ocorrer.	Se o evento de risco ocorrer, impacta somente o próprio processo levemente.
Baixa(o)	O evento de risco tem baixa probabilidade de ocorrer.	Se o evento de risco ocorrer, não impacta nada.

FONTE: Brasiliano, 2015

Neste contexto considera-se que:

1) probabilidade de risco é a chance de que esse risco ocorrerá;

2) impacto do risco é o efeito nos objetivos do processo se o evento de risco ocorrer;

Essas duas dimensões do risco, quando combinadas, resultam em um terceiro elemento denominado *níveis de risco*.

A parametrização dos níveis de risco, mediante a combinação das dimensões probabilidade versus impacto foi arbitrada como se segue:

1) Quadrante 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.

2) Quadrante Laranja - No quadrante II, localizam-se ameaças que poderão ser muito danosas à empresa, podendo possuir muito baixa probabilidade e alto impacto, bem 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 IV é que as ações podem ser implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados.

3) Quadrante Amarelo - No quadrante III estão os riscos com alta probabilidade de ocorrência, mas que causam consequências gerenciáveis à empresa. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de emergência, se for o caso.

4) Quadrante 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, a princípio, estão na zona de conforto.

2.1.4 MATRIZ DE RISCOS

A avaliação de riscos visa comparar os níveis de riscos em relação aos critérios preestabelecidos. 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 organização 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.

A matriz de riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Quanto maior for à probabilidade e o impacto de um risco, maior será o nível do risco.

a) matriz de exposição ao risco probabilidade x impacto

Impacto	Probabilidade				
	Baixa	Média	Alta	Muito Alta	Elevada
Elevado				I	
Muito Alto			II		
Alto		III			
Médio	IV				
Baixo					

Legenda

Ponderação Probabilidade e Impacto:
Elevada: 5
Muito Alta: 4
Alta: 3
Média: 2
Baixa: 1

Níveis de Risco:
- Ação imediata
- Ação média e curto prazo
- Monitoramento e gestão
- Risco controlável

2.1.5 RESPOSTAS AOS RISCOS

É importante que exista a conscientização e comprometimento com o gerenciamento de riscos por parte da administração do Exército. 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.

- **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.

- **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 o gestor da área **decide assumir risco no quadrante laranja**, tendo em vista relação custo-benefício ou por questões estratégicas. **No entanto, não é aceitável a possibilidade de assumir riscos no quadrante vermelho.**

2.1.6 PLANO DE AÇÃO

Depois de identificados, avaliados e mensurados, deve-se definir qual tratamento deve ser atribuído aos riscos. 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; e
- **How Much? (Quanto Custa?):** Qual o valor do investimento.

Exemplo:

O que ocasiona o risco?	Controle	O controle é eficaz?	Quem faz parte neste processo?	Quando será implementado?	O que pode ser implementado?	Como deve ser realizado?	Quanto custa?	Status
REALIZAÇÃO DE PAGAMENTO EM ATRASO								
Entesouramento do numerário sub-repassado	Não possui	Não aplicável	1º Ten Osmar – Encarregado do Setor Financeiro	05/06/16	Controle	Colher assinatura do Ordenador de Despesas nas Relações Externas das Ordens Bancárias até D+1 do dia do sub-repasse	-	
Recolhimento incorreto das alíquotas de impostos	Não possui	Não aplicável	S . Ten Marcos e 1º Sgt Santos - Auxiliares do Setor Financeiro	05/06/16	Controle	Capacitar os auxiliares do Setor Financeiro em Contas a Pagar e a Receber - CPR	R$ 2.000,00	

Figura 3 – Plano de Ação

3. CONSIDERAÇÕES FINAIS

Nas organizações em que o estágio de maturidade com relação a Gestão de Riscos esteja mais avançado, este trabalho pode ser realizado por meio de uma visita de auditoria com a finalidade específica de verificar a infraestrutura de gestão de riscos, os sistemas de controle da organização como um todo, por área ou até processo. A atividade de auditoria deve sempre que possível e à medida que o processo de gestão de riscos esteja adequado e enraizado, se apoiar na visão da organização com relação a riscos.

Nas demais, em que o nível ainda seja incipiente, o Controle Interno promove a Gestão de Riscos e busca se basear na avaliação de riscos da própria auditoria.

Convém destacar que o resultado final de um trabalho desta natureza é assegurar que os riscos estão sendo gerenciados dentro de um nível de aceitação, denominado Apetite por Riscos da Organização.

4. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:** Gestão de riscos – princípios e diretrizes, 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=57311/>.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31010:** Gestão de Riscos – Técnicas para o Processo de Avaliação de Riscos, 2012. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=090516/>.

BRASIL. Ministério da Defesa. Comando do Exército. **Portaria nº 813-Cmt Ex, de 28 de setembro de 2012:** aprova as Normas para a Realização das Atividades de Auditoria e Fiscalização pelo Controle Interno do Comando do Exército (EB10-N-13.003). Boletim do Exército. Brasília, DF, 2012.

_____. Ministério da Defesa. Comando do Exército. **Portaria nº 018-Cmt Ex, de 17 de janeiro de 2013:** aprova o Manual de Auditoria (EB 10-MT-13.001) e dá outras providências. Boletim do Exército. Brasília, DF, 2013.

_____. Tribunal de Contas da União. **Revista do Tribunal de Contas da União número 132, janeiro/abril 2015.** Metodologia de Auditoria com Foco em Processo e Risco. Brasília: TCU, 2015. p. 28. Disponível em: <http://portal.tcu.gov.br/publicacoes-institucionais/periodicos-e-series/revista-do-tcu/>.

BRASILIANO, Antônio Celso Ribeiro. **GESTÃO DE RISCO DE FRAUDE:** Fraud Risk Assessment - FRA. Sicurezza Editora, 2015.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de riscos corporativos**. Tradução Audibra e PricewaterhouseCopers. São Paulo: [s.n.], 2013, 135 p.

DE CICCO, Francesco. **AUDITORIA BASEADA EM RISCOS:** Como implementar a ABR nas organizações: uma abordagem inovadora. Risk Tecnologia Editora Ltda, 2007.

Brasília, DF, 11 de MAIO de 2016.

Gen Div LUIZ ARNALDO BARRETO ARAUJO
Chefe do Centro de Controle Interno do Exército