MINISTÉRIO DA DEFESA
ESCOLA SUPERIOR DE GUERRA
ASSESSORIA DE CONTROLE INTERNO

INSTRUÇÃO NORMATIVA ACI ESG/COMANDO ESG-MD N° 2, DE 24 DE AGOSTO DE 2022

Dispõe sobre a Gestão de Riscos no âmbito da Escola Superior de Guerra.

O COMANDANTE DA ESCOLA SUPERIOR DE GUERRA, no uso da atribuição que lhe confere o inciso III, do art. 121 do Regimento Interno da Escola Superior de Guerra, aprovado pela Portaria nº 1169/GAB ESG/ESG-MD, de 13 de março de 2020, resolve:

Art.1º Instituir a presente Instrução Normativa com a finalidade de estabelecer a estrutura básica, competência e procedimentos para o funcionamento da Gestão de Riscos na Escola Superior de Guerra (ESG).

DISPOSIÇÕES INICIAIS

Art. 2º. A Gestão de Riscos, um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos da ESG, será conduzida pelo CGRC.

TRÊS LINHAS DE DEFESA

Art. 3º. Há três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos, como explanado a seguir:

I - **Funções que gerenciam e têm propriedade de riscos**: a gestão operacional e os procedimentos rotineiros constituem a primeira linha de defesa na gestão de riscos. Os controles internos são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. Nesse nível se identificam, avaliam e mitigam riscos por meio do desenvolvimento e da implementação de políticas e procedimentos internos que possam oferecer garantia razoável de que as atividades estejam de acordo com as metas e objetivos.

II - **Funções que supervisionam riscos**: a segunda linha de defesa é constituída pela Assessoria de Controle Interno para garantir que a primeira linha funcione no que diz respeito à gestão de riscos e controles. Seu papel é coordenar as atividades de gestão de riscos, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional, apoiar a definição de metas de exposição a riscos, monitorar riscos específicos (de compliance, por exemplo), bem como ajudar a definir controles e/ ou monitorar riscos e controles da primeira linha de defesa.

III - **Funções que fornecem avaliações independentes**: a CISET constitui a terceira linha de defesa na gestão de riscos ao fornecer avaliações independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração da ESG.

IDENTIFICAÇÃO DE RISCOS

Art. 4º. A identificação de riscos é uma função do ACI e consiste no processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e apoiando-se na comunicação e consulta com as partes interessadas internas e externas.

Art. 5º. A identificação de riscos em etapa inicial ou preliminar pode adotar uma abordagem de identificação de riscos top-down, que vai do geral para o específico, ou seja, de cima para baixo:

I – Fazer uma listagem e um breve resumo dos objetivos organizacionais, pois são os riscos desses objetivos não serem atingidos, que serão gerenciados.

II - Feito isso, é necessária a montagem da matriz SWOT que serve para mostrar o ambiente no qual os objetivos institucionais serão perseguidos. (S-Strengths (Forças), W-Weaknesses (Fraquezas), O-Opportunities (Oportunidades), T-Threats (Ameaças)).

III - Identificar os riscos em um nível geral ou superior para se estabelecer prioridades.

IV- Identificar e analisar riscos em nível específico e/ou mais detalhado.

V - A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, assim como em necessidades das partes interessadas. A documentação dessa etapa geralmente inclui:

a) o escopo do processo, projeto ou atividade coberto pela identificação;

b) os participantes do processo de identificação dos riscos;

c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas; e

d) descrição de cada risco, pelo menos com a fonte de risco, as causas, o evento e as consequências.

VI - Uma vez feito o mapeamento e a listagem dos eventos de riscos, é necessário listar as possíveis causas e consequências de cada um desses eventos, para fecharmos a etapa de identificação de riscos.

ANÁLISE DE RISCOS

Art. 6º. É o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos.

Art. 7º. O nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos.

Art. 8º. O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco.

Art. 9º. Cabe ao ACI identificar os fatores que afetam a probabilidade e as consequências, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco, expressas em termos tangíveis ou intangíveis.

Art. 10º. Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas, e ser mais ou menos detalhada.

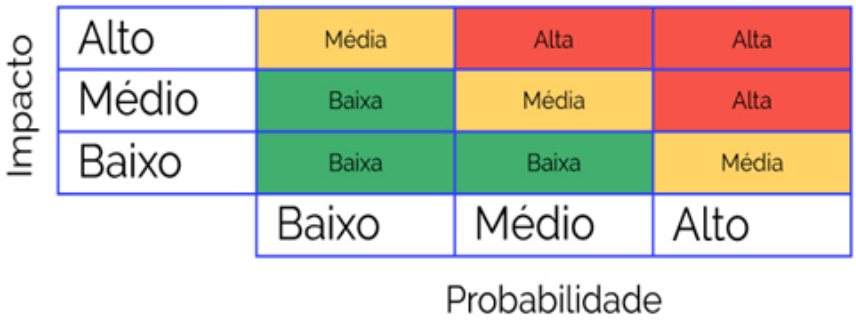
I - Métodos qualitativos definem o impacto, a probabilidade e o nível de risco por qualificadores como “alto”, “médio” e “baixo”, com base na percepção das pessoas.

II - Métodos semiquantitativos usam escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco. A escala pode ser linear, logarítmica ou de outro tipo.

III - Métodos quantitativos estimam valores para as consequências e suas probabilidades a partir de valores práticos e calculam o nível de risco a partir de unidades específicas definidas no

desenvolvimento do contexto.

IV - Em sua forma qualitativa mais elementar, a relação entre os riscos e os seus componentes pode ser ilustrada por meio de uma matriz simples, como a que segue:



Quadro 1: EXEMPLO DE ESCALA DE PROBABILIDADES (BRASIL, 2012, adaptado).

Descritor	Descrição	Nível
Muito Baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	1
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito Alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Quadro 2: EXEMPLO DE ESCALA DE CONSEQUÊNCIAS (BRASIL, 2012, adaptado).

Descritor	Descrição	Nível
Muito Baixo	**Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação/ comunicação / divulgação ou de conformidade).	1
Baixo	**Pequeno** impacto nos objetivos (idem)	2
Médio	**Moderado** impacto nos objetivos (idem), porém recuperável	5
Alto	**Significativo** impacto nos objetivos (idem), de difícil reversão	8
Muito Alto	**Catastrófico** impacto nos objetivos (idem), de forma irreversível	10

AVALIAÇÃO DE RISCOS

Art. 11º. A finalidade da avaliação de riscos é 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.

Art. 12º. Nessa etapa, o ACI fará uso da compreensão e do nível dos riscos obtidos na etapa de análise de riscos para tomar decisões acerca dos riscos analisados, em especial:

I - Se um determinado risco precisa de tratamento e a prioridade para isso.

II - Se uma determinada atividade deve ser realizada ou descontinuada.

III - Se controles internos devem ser implementados ou, se já existirem, se devem ser modificados, mantidos ou eliminados.

Art. 13º. Ao CGRC cabe estabelecer critérios para priorização e tratamento associados aos níveis de risco como nível recomendado de atenção, tempo de resposta requerido, e quem deve ser comunicado.

Critérios para priorização e tratamento de riscos:

I – RE: Nível de risco muito além do apetite a risco. Requer uma resposta imediata. Postergação de medidas só com autorização do Comandante.

II – RA: Nível de risco além do apetite a risco. Requer uma ação tomada em período determinado. Postergação de medidas só com autorização do Comandante.

III - RM: Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.

IV - RB: Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Parágrafo Único: A documentação desta etapa é importante instrumento de accountability e consiste em uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

TRATAMENTO DE RISCO

Art. 14º. O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. Opções de tratamento de riscos incluem evitar, reduzir (mitigar), transferir (compartilhar) e aceitar (tolerar) o risco, devendo-se observar que elas não são mutuamente exclusivas.

Art. 15º. Mitigar os riscos preparando por meio da gestão da continuidade operacional. Avaliar essa opção de tratamento quando ocorrem as seguintes condições:

I - O objeto da gestão é atividade ou processo crítico da organização, portanto o impacto é muito alto.

II - O evento de risco tem baixa probabilidade, o que poderia levar à falsa impressão de que o nível do risco poderia ser tolerado após a implantação de controles preventivos.

Art. 16º. Ao avaliar os efeitos das diferentes respostas possíveis, a gestão decide a melhor forma de tratar o risco. A resposta ou combinação de respostas selecionadas não precisa necessariamente gerar a quantidade mínima de risco residual, mas se gerar um risco residual acima dos limites de exposição estabelecidos, os gestores terão que reconsiderar a opção de resposta ou rever os limites.

O processo de tratamento é cíclico e inclui:

I - Avaliar o tratamento já realizado.

II - Avaliar se os níveis de risco residual são toleráveis.

III - Se não forem, definir e implementar o tratamento adicional.

IV - Avaliar a eficácia desse tratamento.

Art. 17º. Solicitar o registro de riscos da organização desta etapa, bem como identificar:

I - As razões para a seleção das opções de tratamento, incluindo os benefícios esperados.

II - Os responsáveis pela aprovação e pela implementação do plano.

III - As ações propostas, os recursos requeridos, incluindo arranjos de contingência, e o cronograma.

IV - As medidas de desempenho e os requisitos para prestação de informações.

V - As formas de monitoramento da implementação do tratamento e dos riscos.

MONITORAMENTO E ANÁLISE CRÍTICA

Art. 18º. O CGRC fará o monitoramento e a análise crítica da gestão de riscos com a finalidade de:

I - Detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes.

II - Obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos.

III - Analisar eventos (incluindo os “quase incidentes”), mudanças, tendências, sucessos e fracassos e aprender com eles.

IV - Assegurar que os controles sejam eficazes e eficientes no projeto e na operação.

Art. 19º. A seguir irá definir e detalhar as responsabilidades relativas ao monitoramento e a análise crítica na política e detalhadas nos planos, manuais ou normativos da gestão de riscos que contemplam atividades como:

I - Monitoramento contínuo (ou pelo menos, frequente) pelas funções que gerenciam e têm propriedade de riscos e pelas funções que supervisionam riscos, com vistas a medir o desempenho da gestão de riscos, por meio de indicadores chave de risco, análise do ritmo de atividades, operações ou fluxos atuais em comparação com o que seria necessário para o alcance de objetivos ou manutenção das atividades dentro dos critérios de risco estabelecidos.

II - Análise crítica dos riscos e seus tratamentos realizada pelas funções que gerenciam e têm propriedade de riscos e/ou pelas funções que supervisionam riscos, por meio de autoavaliação de riscos e controles (Control and Risk Self Assessment - CRSA).

III - Auditorias realizadas pelas funções que fornecem avaliações independentes, focando na estrutura e no processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez de situações específicas.

Parágrafo Único: As atividades de monitoramento e análise crítica devem assegurar que o registro de riscos seja mantido atualizado, bem como que nele sejam documentados os resultados das ações mencionadas acima.

TÉCNICAS PARA GESTÃO DE RISCOS

Art. 20º. O ACI utilizará a matriz de riscos, conhecida como "matriz de probabilidade/consequência" e que constitui apenas uma das possíveis técnicas que podem ser utilizadas para auxiliar a identificação, análise e avaliação de riscos.

Art. 21º. Exige a atuação de um facilitador, que deve provocar a participação das pessoas a partir de perguntas previamente elaboradas do tipo "e se", "o que aconteceria se", "alguém ou algo pode ...?", "alguém ou algo nunca...?".

Art. 22º. Outra técnica que poderá ser usada pelo ACI, de acordo com a necessidade será a ANÁLISE BOW TIE - técnica que busca analisar e descrever os caminhos de um evento de risco, desde suas causas até as consequências, por meio de uma representação pictográfica semelhante a uma gravata borboleta (bow tie). O método tem como foco as barreiras entre as causas e o evento de risco e as barreiras entre o evento de risco e suas consequências.

I – CAUSAS: fragilidades ou ameaças que podem propiciar a ocorrência do evento.

II – CONSEQUÊNCIAS: possíveis efeitos resultantes da ocorrência do evento.

DISPOSIÇÕES FINAIS

Art. 23º. Esta Instrução Normativa entra em vigor na data de sua publicação em Boletim.

Art. 24. Fica revogada a Portaria nº 1185/ACI ESG/ESG-MD, de 11 de março de 2020.

General de Divisão ADILSON CARLOS KATIBE

Comandante da ESG