Esta es una fiel traducción y copia del documento original en español.

Carlos Julio Carrero
Traductor Oficial Português-Español
Resolución No. 0271
Agosto 18, 2008

1. OBJETIVO

Oferecer diretrizes para a aplicação do ciclo de gerenciamento de riscos em nível dos processos, de modo a garantir a gerenciamento adequada desses riscos e produzir informações confiáveis para a tomada de decisões na Ecopetrol S.A. e nas empresas do Grupo Ecopetrol que consolidam as demonstrações financeiras.

2. CONDIÇÕES GERAIS

As diretrizes para a Gerenciamento de Riscos de Processos são estabelecidas pela Direção Corporativa de Asseguramento do Controle Interno para serem cumpridas pela Ecopetrol S.A. e pelas empresas do Grupo[1]. Estas diretrizes são detalhadas neste documento e devem ser executadas através do cumprimento do ciclo para a gerenciamento de riscos[2] a nível de processos.

O processo de gerenciamento de risco é baseado no Ciclo de Gerenciamento de Risco que é comum a todas as metodologias e estruturas do gerenciamento de riscos, que abrange as fases de planejamento, identificação, avaliação, tratamento, monitoramento e comunicação, conforme demonstrado a seguir:

Figura 1. Ciclo de gerenciamento de riscos

[1] Para as empresas do Grupo, devem ser consideradas sua dimensão e realidade operacional.

[2] Ao longo deste documento, o termo Processo significará todos aqueles contidos no Mapa Oficial de processos da Empresa, incluindo os Sistemas de Gestão.

Para efeitos de aplicação do Ciclo de Gerenciamento de Riscos na Ecopetrol S.A. e no seu Grupo Empresarial, o termo Risco faz referência a qualquer evento de ocorrência incerta que, se acontece, gera um impacto negativo[3] no alcance ou cumprimento dos objetivos e processos da empresa, e pode ser medido em termos da probabilidade de ocorrência das causas e do impacto das consequências.

O sucesso do gerenciamento de riscos depende da aplicação deste procedimento, cujas atividades devem ser realizadas, pelo menos, uma vez por ano.

3. DESENVOLVIMENTO

O ciclo de gerenciamento de riscos em processos é aplicado, pelo menos, uma vez por ano e cada vez que é necessário, de acordo com a natureza do processo, e é cumprido através das fases seguintes:

3.1 FASE 1 - ELABORAÇÃO DO PLANO DE TRABALHO

É necessário um plano de trabalho anual com atividades anuais e recorrentes para assegurar a gerenciamento adequada dos riscos nos processos, de modo a definir o escopo, os recursos, o tempo, as diretrizes e as ferramentas necessárias para desenvolver as atividades inerentes à gerenciamento dos riscos nos processos.

[3] O alcance positivo do risco é desenvolvido através dos processos de definição da estratégia, da análise de aproveitamento das oportunidades para que as metas do negócio ou dos processos possam ser atingidas.

3.1.a **Entradas**

- *Informações do Processo*: Mapa de processos, objetivo e escopo do processo sob análise, fluxos de atividades dos subprocessos, interações e atributos (entradas, saídas, documentos, indicadores, entre outros)

- *Lições aprendidas*: Experiências, avaliações e oportunidades de melhoria detectadas na aplicação anterior do Ciclo de Gerenciamento de Riscos.

- *Outros insumos*: Diretrizes e procedimentos organizacionais que podem influenciar o planeamento da gerenciamento de riscos. Eles podem incluir níveis de autoridade e tomada de decisões, entre outros.

3.1.b **Processo**

Com base no cronograma delineado pela Direção Corporativa de Asseguramento do Controle Interno da Ecopetrol S.A., cada área/empresa deve definir um plano de trabalho incluindo datas determinadas.

As atividades deste plano devem estar alinhadas com as atividades descritas neste procedimento e devem contar com a(s) pessoa(s) responsável(eis), data de início e fim, resultados, recursos necessários, ferramentas para definir como as informações são registradas e analisadas em cada uma das etapas, definição de como os resultados serão divulgados às partes interessadas, internas e externas, entre outros.

Dentro da definição dos membros da equipe de trabalho, deve haver pessoal especializado nas diferentes áreas para garantir que os riscos, medidas de mitigação e alarmes de risco sejam identificados com detalhes suficientes. A equipe de trabalho deve necessariamente incluir os executores do processo, especialistas técnicos e um profissional em Riscos e Controle Interno ou quem quer que esteja atuando como tal nas empresas.

3.1.c **Saídas**

No final desta fase, deve estar disponível um plano de trabalho anual de gerenciamento de riscos para cada processo da Ecopetrol e para cada empresa, nos formulários definidos para isso. Esse plano de trabalho deve ser divulgado antecipadamente e, sempre que necessário, enviado aos participantes no ciclo de gerenciamento de riscos na(s) área(s) envolvida(s).

3.2 FASE 2 - COMPREENSÃO DO PROCESSO

Sempre que os riscos e suas medidas de mitigação e alarmes precisarem ser identificados, documentados e geridos, será necessário fazer previamente uma análise do processo que estará sujeito a revisão, de modo a compreender em detalhes as atividades, interações, resultados e outras informações relevantes para o exercício. Para documentar este exercício, deve ser preenchido o formulário GEE-F-043 "Formulário do Papel de Trabalho de Construção da Matriz de Riscos e Controles".

3.2.a **Entradas**

- *Informação do Processo*: Descrição do processo e dos objetivos, da forma de aplicar o processo, escopo e limitações do escopo do processo em relação ao objetivo do processo, mudanças reais ou potenciais na criação do processo (transição), atividades, interações internas ou externas, papéis e responsabilidades, resultados, transações, informação e sistemas de informação do processo, eventos ou situações que possam gerar falhas no processo, falhas apresentadas dentro da operação e no resultado do processo, terceiros relevantes do processo, relação de contas significativas para os processos, entre outros.

- *Informações sobre os objetivos*: Objetivos do processo e objetivos estratégicos associados ao processo (extraídos das Tabelas Balanceadas de Gerenciamento -TBG- das áreas relacionadas com o processo), partes envolvidas no cumprimento do objetivo, forma de medição do cumprimento do objetivo, fatores críticos de sucesso para atingir o objetivo, insumos críticos para o desempenho do processo, entre outros.

3.2.b **Processo**

Para compreender a sequência lógica do processo e a informação relacionada com o funcionamento do processo: O que faz o processo? Para que serve? Com que processos interage? Quais os principais resultados?, entre outros;
Revise como opera o processo, compreenda seus objetivos e escopo, suas entradas, atividades de transformação e as saídas. Além disso, devem ser identificadas suas interações com outros processos e outros dados de entrada no numeral 3.2.a e, diante dessa compreensão, analisar pelo menos:

- Se o processo teve mudanças significativas que tenham gerado um impacto no sistema de controle interno (por exemplo: escopo, funções e responsabilidades, atividades críticas, transações financeiras, sistemas de informação, entre outros).
- Se há limitações no seu escopo em relação aos objetivos dos mesmos. Caso haja limitações no escopo, elas devem ser claramente documentadas no exercício de compreensão do processo.
- Que eventos ou situações internas ou do entorno, potenciais ou reais, ocorrem causando possíveis falhas no processo.
- Que situações do processo levaram à identificação de problemas nas autoavaliações, nos monitoramentos preventivos, nas análises da gerência e em outras auditorias, especialmente considerando situações recorrentes e, pelo menos, os problemas que tenham sido detectados nos seis meses anteriores à análise realizada.
- A identificação[4] dos terceiros relevantes que interagem no mesmo (empreiteiras que prestam serviços relevantes que fazem parte dos processos, cuja execução poderia afetar o Sistema de Controle Interno).
- A associação ao processo de transações e contas significativas das demonstrações financeiras com base nas definições de contas e processos significativos realizados anualmente pela Direção Corporativa de Asseguramento do Controle Interno.
- A identificação dos sistemas de informação críticos e relevantes para a execução e o desenvolvimento do processo.
- O alinhamento dos objetivos do processo e o seu cumprimento com os objetivos estratégicos do(s) TBG(s) das áreas que se relacionam com o processo que estiver sob análise.
- A forma de medição do cumprimento dos objetivos e os fatores críticos de sucesso para atingir o objetivo.
- A segregação de funções das atividades, papéis e responsabilidades, e sistemas de informação relacionados com o processo.

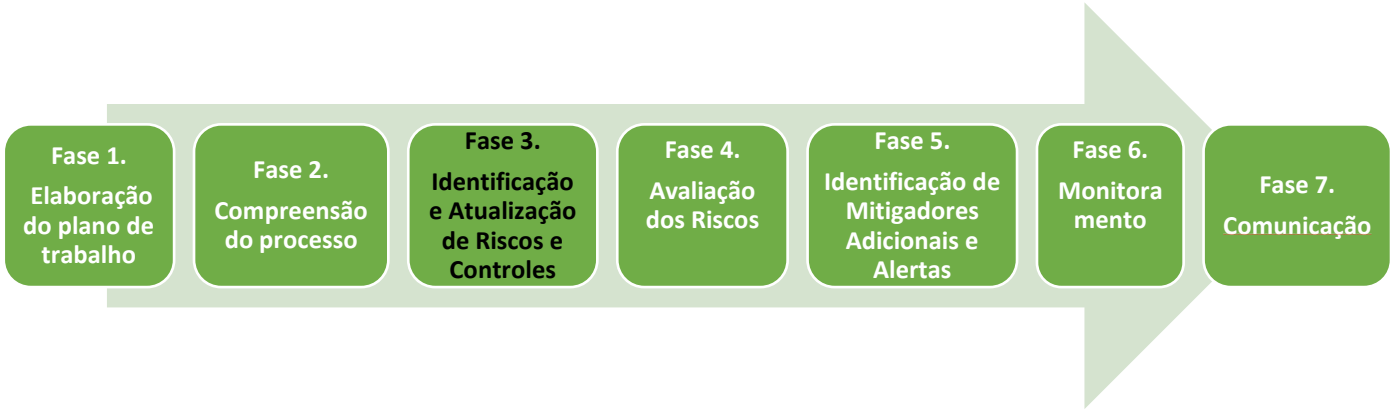
3.2.c **Saídas**

No final desta fase, deve haver compreensão suficiente do processo para fazer a análise dos riscos e dos controles. Além disso, deve ser conhecido o panorama completo dos objetivos (estratégicos e processuais) relacionados com a matriz de riscos e controles.

[4] Para a identificação de terceiros relevantes (Organizações Prestadoras de Serviços da OPS), preencha o GEE-F-043 "Formulário Papel de Trabalho Construção da Matriz de Riscos e Controles".

3.3 FASE 3 - IDENTIFICAÇÃO E ATUALIZAÇÃO DE RISCOS E CONTROLES

A identificação dos riscos permite, de forma sistemática e estruturada, determinar os eventos que podem afetar negativamente os objetivos (estratégicos, operacionais, de reporte, de conformidade) do processo. Estes eventos devem ser considerados, quer estejam ou não sob o controle da organização. Além disso, a associação e atualização dos controles permite fazer um exercício de avaliação e tratamento mais próximo da realidade operacional do processo.



3.3.a **Entradas**

- *Informação do processo*: Mapa vigente de processos; resultados da compreensão do processo realizado.
- *Informação dos objetivos*: Alinhamento dos objetivos do processo com os objetivos estratégicos dos TBG das áreas associadas ao processo e seus indicadores, resultados dos indicadores de objetivos estratégicos e do processo do período anterior, fatores do entorno que podem afetar o escopo dos objetivos.
- *Informações sobre os riscos* e *medidas de mitigação*: Matriz de riscos e controles dos processos[5], matriz de implantação de Riscos Empresariais nos processos vigentes, relatório de eventos ocorridos atualizado, resultados recentes de autoavaliações, resultados dos testes da direção, resultados das questões que tenham sido detectadas nos últimos seis meses de monitoramento preventivo e auditorias internas e externas que afetam a matriz de riscos e controles, e as diretrizes para a identificação e a documentação dos riscos e controles de processos vigente.
- *Outros:* Resultados organizacionais, mudanças regulatórias, mudanças tecnológicas, iniciativas ou projetos em andamento, entre outros que podem ter influência na gerenciamento de riscos do

[5] Caso a Matriz de Riscos e Controles esteja disponível, ela deve ser considerada durante o exercício.

processo/empresa, regulamentações que impactam na implantação dos riscos e nas medidas de mitigação (por exemplo, ISO 37001 - Sistema de Gerenciamento Antissuborno).

3.3.b **Processo**

a. IDENTIFICAÇÃO/ATUALIZAÇÃO DOS RISCOS

Para novos processos ou processos que tenham mudanças significativas para que um novo exercício de gerenciamento de riscos possa ser realizado, devem ser identificados os riscos que podem ter impacto no escopo dos objetivos previamente analisados.

Caso contrário, se for um exercício de atualização, devem ser previamente identificados os riscos e verificar a sua validade e suficiência em relação à cobertura dos objetivos do processo.

Em ambos os casos, é necessária a utilização do formulário GEE-F-043 "Formulário do Papel de Trabalho de Construção da Matriz de Riscos e Controles" para garantir a execução do exercício[6].

b. DEFINIÇÃO DE RISCOS

Os riscos devem ser definidos por três elementos: Evento, causas e consequências[7].

*Definir o Evento***:** O evento deve ser redigido como a situação que, se ocorrer, gerará um impacto negativo no alcance ou cumprimento dos objetivos dos processos. Para identificá-los, selecione o objetivo analisado e se pergunte que situação poderia acontecer que causaria que o objetivo não seja atingido. Ele não deve ser escrito como a negação do objetivo, nem como a não execução das atividades do processo. Portanto, evite usar termos como "Inadequado, Insuficiente, Não garantir".

*Estabelecer as causas***:** Faz referência ao porquê de um evento deste tipo poderia acontecer. Deve ser realizada a análise das causas diretas, sejam elas internas ou do entorno que dá origem ao evento, incluindo as que são controladas diretamente no âmbito do processo e as que não, levando em conta que é nessas causas que serão aplicadas as medidas de mitigação do risco (controles ou ações de tratamento), portanto, estas devem ser concretas e coerentes.

*Estabelecer as Consequências***:** Qual seria o impacto da ocorrência do evento de risco nos recursos (pessoas, ambiente, economia, reputação, entre outros)?
Devem ser determinadas as consequências diretas.

A definição dos riscos pode ser feita utilizando as seguintes técnicas:

- Brainstorming: Consiste em reunir a equipe de trabalho definido, de modo que cada participante exponha o que considera serem os riscos que afetam os objetivos do processo e, posteriormente, fazer uma análise e consolidação.

[6] Para a Ecopetrol, a folha de identificação deste formulário deve ser documentada. Para as empresas, é utilizado o formulário que desenvolve cada empresa para este fim.
[7] Para a definição de riscos de conformidade, consulte o Anexo 3 deste documento.

- Sondagens: consiste na aplicação de questionários abertos ou de uma lista de verificação dos riscos previamente identificados. É prático quando a equipe de trabalho é grande ou dispersa e fica difícil aplicar outras técnicas.

- Entrevistas: Consiste em um diálogo estruturado através de perguntas e respostas. Tem a vantagem de permitir ter acesso à opinião de um especialista com disponibilidade restrita ou obter maior qualidade por não ser tendencioso em uma sessão de grupo. Na entrevista, o objetivo é conhecer as opiniões em relação aos riscos do processo. É útil para obter informações em primeira mão dos especialistas.

- Outras ferramentas: Alternativas como lista de categorias de riscos por negócio, técnicas de diagramação (causa-efeito, espinha de peixe, diagramas de influência), análise DOFA, técnica Delphi, entre outras.

Embora as técnicas de identificação não garantam por si só uma identificação absoluta, deve ser feita uma análise suficiente dos riscos identificados deve ser feita em função dos objetivos e do escopo do processo.

Para isso, a identificação ou atualização dos riscos deve levar em conta que:

- Os riscos sejam significativos em seu possível efeito no atingimento do objetivo.
- Um risco pode ser associado a vários objetivos.
- Os riscos devem ser suficientes para cobrir o escopo do objetivo do processo.
- Sejam definidas apenas as causas diretas do evento de risco (não a causa da causa).
- Sejam incluídas sempre as causas internas e externas aplicáveis ao processo.
- Sejam consideradas e resolvidas as observações relativas aos riscos do processo decorrentes de autoavaliações, monitoramento, testes da gerência e outras auditorias internas e externas.
- Todos os objetivos (estratégicos, operacionais, de reporte, de Conformidade) dos processos sejam abrangidos e que incluam o funcionamento do processo para os casos em que tenham sido identificadas limitações no escopo do processo em relação aos objetivos estabelecidos.
- Os riscos empresariais estejam incluídos de acordo com a matriz de riscos do negócio contra os processos[8]
- Os fatores de risco de suborno sejam incluídos, de acordo com o previsto na norma ISO 37000.
- Se o risco estiver dentro do escopo de outro processo, ele seja incluído na matriz do processo que corresponder.
- Devem ser determinados os pontos do processo em que existem riscos não identificados que podem ter impacto no funcionamento normal e no cumprimento dos objetivos do processo e que não tenham sido evidenciados nas etapas anteriores.
- Sejam considerados os eventos de risco empresariais que possam gerar um impactar nos objetivos do processo que está sendo analisado.
- Se o processo em análise tiver limitações no seu delineamento ou escopo (há diferenças entre o que é escrito e o que é feito no processo, que não haja suficientes atividades concebidas ou documentadas, que não haja interações suficientes com outros processos, que esteja em processo de documentação ou de mudança/transição, entre outros), certifique-se de identificar os riscos que

[8] Se a empresa já desenvolveu a relação entre os riscos empresariais e os do processo

tenham suficiente escopo para que todo o processo seja coberto, independentemente do estatuto do desenho do processo.

c. CLASSIFICAÇÃO DOS RISCOS

Os riscos identificados devem ser classificados de acordo com a categoria do evento, de acordo com os seguintes critérios:

- **Estratégico**: Risco associado aos objetivos estratégicos da área ou da empresa, ou aqueles riscos que tenham sido identificados segundo a matriz de riscos empresariais contra os processos.
- **Financeiro:** Risco cuja ocorrência afeta diretamente a confiabilidade e a razoabilidade dos números das demonstrações financeiras.
- **Conformidade**: Risco associado ao não cumprimento das leis e dos regulamentos aplicáveis à empresa, com ênfase na fraude, apropriação indevida de ativos, corrupção, suborno, denúncia de fraude, branqueamento de capitais, financiamento do terrorismo, FCPA.
- **Operacional:** Riscos diretamente relacionados com a realização do processo, devido a causas internas ou externas.

As categorias não são excludentes entre si, portanto, um risco pode ser classificado em uma ou mais categorias.

d. IDENTIFICAÇÃO/ATUALIZAÇÃO DOS CONTROLES E OUTROS MITIGADORES

Nesta fase, são analisadas as causas a serem geridas para cada um dos riscos e, a partir daí, são identificadas as medidas de mitigação que permitem reduzir a probabilidade. Da mesma forma, as consequências do risco são analisadas e se identificam as medidas que podem reduzir o impacto.

Para um processo cujos riscos tenham sido recentemente estabelecidos, deve ser realizado um novo exercício de identificação de controles, começando com as causas dos riscos identificados.

Para um exercício de atualização, é necessário partir dos controles previamente estabelecidos e conferir sua validade e suficiência em relação à cobertura dos riscos do processo. Isto é feito alinhando primeiro as causas diretas do risco com os controles existentes.

Em ambos os casos, a utilização do formulário GEE-F-043 "Formulário do Papel de Trabalho de Construção da Matriz de Riscos e Controles" é necessária para garantir a traçabilidade do exercício.

e. DEFINIÇÃO DE CONTROLES E OUTROS MITIGADORES

A definição de controles e ações de tratamento deve ser realizada de acordo com o previsto no "Procedimento de Gerenciamento de Controles e Medidas de Mitigação", GEE-P-006.

Um agente mitigador existente deve ser modificado, entre outras coisas, quando:

- Não está alinhado com as causas diretas do risco associado.
- Há mudanças no funcionamento do mitigador ou do processo associado.
- Não mitiga a causa associada.
- Existem recomendações derivadas de autoavaliações, monitoramentos, testes da gerência e outras auditorias internas e externas sobre a sua concepção/operação.
- A ação de mitigação não foi aplicada ou não é eficaz.
- Há mudanças no escopo, nos responsáveis, nas datas de início ou fim, na ação de mitigação.

É importante destaca que, para os mitigadores existentes que são atualizados, seus atributos também devem ser atualizados para garantir a consistência, isto é, analisar se a modificação da ação de mitigação gera mudanças no executor, frequência, tipo, classificação, entre outros fatores.

3.3.c **Saídas**

No final desta etapa, o formulário GEE-F-043 " Formulário do Papel de Trabalho de Construção da Matriz de Riscos e Controles" deve ser obtido com os riscos associados aos objetivos do processo e os controles e outros agentes mitigadores correspondentes aos riscos abordados e previamente validados pelos proprietários do processo.

3.4 FASE 4 - AVALIAÇÃO DOS RISCOS

A avaliação de riscos é baseada em uma análise semi-quantitativa que procura priorizar os riscos lhes atribuindo valores dentro de escalas ou faixas de probabilidade e impacto predefinidos.

Os riscos devem ser priorizados de modo a alcançar uma distribuição eficaz dos recursos disponíveis para fazer frente a esses riscos críticos. Isto é possível através da estimativa da probabilidade de ocorrência do evento e do impacto das suas consequências nos recursos (pessoas, ambiente, economia, reputação, clientes, entre outros[9]).

[9] Como definido para cada uma das empresas.

O exercício de avaliação é realizado com base nos riscos identificados, documentando-os no Formulário de Avaliação dos Riscos estabelecido para esse fim[10], no qual o resultado da avaliação deve ser registrado e considerando duas instâncias principais: a avaliação inerente e a avaliação residual, conforme se mostra na figura a seguir:

Figura 2: Avaliação Inerente e Residual

3.4.a **Entradas**

- *Informações sobre riscos e medidas de mitigação*: Definição de apetite ao risco (definida na Matriz de Avaliação dos Riscos da empresa - RAM), formulário de avaliação dos riscos, matriz de riscos e controles dos processos, matriz de riscos e controles transversais e de múltiplos executores,[11]resultados das ações de tratamento e resultados de indicadores-chave de risco (KRI's) do último ano, lista de contas significativas de processos.

- *Informações resultantes* da *gerenciamento de riscos e controles*: Análise de autoavaliações, resultados de testes de controle realizados através dos monitoramentos preventivos, resultados dos Testes da Gerência e das auditorias internas e externas, realizadas nos processos.

- *Outros*: Informações contextuais e ambientais relacionadas aos riscos do processo, tais como projeções de mudanças regulatórias, mudanças tecnológicas, iniciativas ou projetos em andamento, entre outras, informações históricas de incidentes ou riscos ocorridos que permitam a estimativa da frequência de ocorrência e os impactos (dentro dessas informações existem bases de dados de acidentes, custos e tempos, incidentes ocorridos na indústria ou na empresa, mesmo não estando registrados em bases de dados formais).

3.4.b **Processo[12]**

A avaliação dos riscos é realizada durante a execução do ciclo e deve, pelo menos, ser revisada e, se necessário, repetida cada vez que ocorre um evento de risco, quando aparecerem falhas de controle,

[10] O formulário SCI-F-005 aplica-se para avaliação de risco de processo na Ecopetrol S. A. As empresas com mais ou menos recursos ou descritores devem fazer a correspondente adaptação do referido formulário.
[11] Se uma matriz de riscos e controles estiver disponível, os Executadores Transversais e Múltiplos devem ser considerados durante o ano.
[12] Para a Ecopetrol S. A., deve ser aplicado o formulário da Matriz de Avaliação de Riscos, SCI-F-005.

quando as ações de tratamento associadas sejam ineficazes ou canceladas e quando os mitigadores não sejam suficientes.

a. AVALIAÇÃO INERENTE

A avaliação inerente é a avaliação dos riscos baseada na medição da probabilidade e do impacto, sem levar em conta o efeito dos mitigadores.

Para estimar a probabilidade, com base nos descritores de probabilidade definidos na matriz RAM da empresa, é necessário identificar o nível de probabilidade de que um risco se materialize.

Para isso, devem ser analisadas as informações históricas dos eventos ocorridos ou as estatísticas de risco a serem avaliados que tenham ocorrido no setor, empresa ou processo e devem ser identificadas as situações reais mais críticas ou representativas. Se não houver informações suficientes para estabelecer uma situação real, deve ser estruturada uma situação hipotética de forma credível, com base no evento de risco e nos impactos da sua ocorrência nos objetivos estabelecidos.

A situação definida deve ser delimitada por dados numéricos, para facilitar e especificar o valor do cenário. Com base no acima exposto, o cenário ou situação é documentada e com base nela será realizada a avaliação inerente do risco no formulário utilizado para a avaliação dos riscos.

Leve em conta que o cenário deve ser preferencialmente baseado na pior situação histórica conhecida. Para a construção de um cenário hipotético, recomenda-se a revisão com os pares na indústria e criá-lo com os proprietários do processo, os gerentes ou chefes da área relacionada com o risco em estudo, para garantir que o cenário corresponda a situações críticas de acordo com a opinião do especialista no processo.

Se houver informações para a construção de cenários hipotéticos como se fossem reais, deve-se dar prioridade ao cenário real, desde que ele ofereça informações suficientes para executar o exercício de avaliação.

Com base no cenário de avaliação definido, o valor da probabilidade que melhor se adapta ao evento do risco deve ser selecionado, levando em conta as informações disponíveis sobre frequência ou probabilidade. Posteriormente, os impactos da matriz RAM (Pessoas, Ambiente, Recursos Econômicos, Reputação, Clientes, segundo o estabelecido na Matriz de Avaliação da Empresa) são avaliados de acordo com o impacto que geram, levando em conta os efeitos diretos sobre os recursos desta matriz. Para isso, identifique dentre os descritores aquele que melhor refletir o impacto do cenário, analisando cada uma das variáveis aplicáveis de acordo com o cenário.

A avaliação inerente do risco é dada pela combinação da probabilidade e o maior impacto.

b. AVALIAÇÃO RESIDUAL

A avaliação residual é entendida como o nível de risco resultante, quando os mitigadores sobre a probabilidade de ocorrência e os impactos nos recursos são aplicados. É realizada de forma a estabelecer o nível de exposição aos riscos identificados, considerando a existência dos agentes mitigadores que operam e sua eficácia na mitigação dos mesmos.

Uma vez obtida a avaliação inerente do risco, é feita a avaliação residual, com base na suficiência e na suficiência e efetividade do conjunto de fatores mitigadores associados ao risco (controles e ações de tratamento completados com verificações de eficácia).

A classificação dos controles é dada pelos fatores de (a) suficiência dos mitigadores, (b) classificação do controle, (c) apagar controle e (d) eficácia do controle.

a) *Suficiência dos agentes mitigadores*: Associar todos os mitigadores do risco e avaliar se eles são suficientes para controlar as causas, conforme estabelecido no Procedimento de Gerenciamento de Controles e Ações de Tratamento no Grupo Ecopetrol, GEE-P-006. Caso os controles associados não sejam suficientes, entende-se que eles não têm incidência na redução do impacto e da probabilidade.

b) *Classificação do controle:* É baseada na classificação dos controles preventivos, detectores ou corretivos, de acordo com a seguinte associação:

Controle Preventivo	Mitiga as causas do risco
Controle de detectives	Mitiga as causas e/ou reduz os impactos do risco
Controle corretivo	Mitiga ou reduz os impactos do risco

c) *Categoria de controle*: Indique se o controle é automático, manual ou manual dependente de TI, de acordo com o que tenha sido definido na matriz de risco e controles.

d) *Eficácia do Controle*: Estabelecer a eficácia de cada um dos controles com base nos resultados obtidos na Revisão Fiscal, nos testes da gerência, nas autoavaliações do controle interno e no acompanhamento preventivo do controle interno e auditorias, indicando se a ineficácia corresponde à operação ou à concepção.

Com base na combinação dos fatores acima, é atribuída uma pontuação máxima de 100 pontos possíveis para cada controle associado, de acordo com a seguinte estrutura

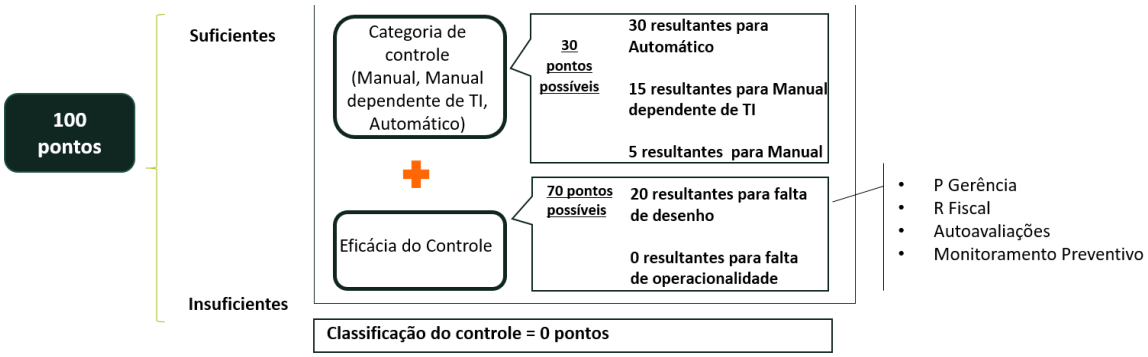


Figura 3. Esquema de pontuação dos controles

A classificação resultante irá determinar se o controle é fraco, moderado ou forte:

- Controle forte: Controle com pontuação de 90 pontos e acima.
- Controle moderado: Controle com pontuação entre 75 e 89 pontos.
- Controle fraco: Controle com 74 pontos ou menos.

Para avaliar o controle com base na classificação ou na pontuação obtida, deve se analisar em que medida o controle gera a probabilidade ou o impacto do risco, levando em conta que:

- Um controle diminui a probabilidade diretamente se a atividade de controle gerencia diretamente a causa associada com o risco.
- Um controle não diminui a probabilidade se a atividade de controle não mitigar a causa do risco.
- Um controle diminui o impacto diretamente se a atividade de controle for destinada a diminuir diretamente um ou mais dos impactos do risco.
- Um controle diminui o impacto indiretamente se a atividade de controle puder diminuir um dos impactos do risco até certo ponto no caso de materialização.
- Um controle não diminui o impacto se a atividade de controle não reduzir o impacto do risco.

Finalmente, de acordo com a avaliação feita para cada controle, o nível de deslocamento do risco inerente deve ser identificado em função do número de colunas e filas de acordo com a tabela a seguir:

Qualificação de controle	Ajuda a diminuir a probabilidade	Ajuda a diminuir o impacto	# Colunas na matriz de risco que se move no eixo da probabilidade	# Colunas na matriz de risco Se movendo no eixo do impacto
Forte	diretamente	diretamente	2	2
Forte	diretamente	indiretamente	2	1
Forte	diretamente	não diminui	2	0
Forte	não diminui	diretamente	0	2
Moderado	diretamente	diretamente	1	1
Moderado	diretamente	indiretamente	1	0
Moderado	diretamente	não diminui	1	0
Moderado	não diminui	diretamente	0	1

Em resumo, o deslocamento do risco inerente no mapa de calor ou na matriz RAM dependerá da média dos níveis de probabilidade e do impacto resultante da aplicação da análise anterior a cada controle, obtendo-se assim o risco residual.

NOTA: Deve se levar em conta que, se o controle a ser avaliado é novo, devido à substituição de um controle racionalizado sobre o qual foram identificadas falhas nos exercícios de monitoramento (auditorias internas ou externas, testes da gerência, autoavaliações de controle interno, entre outros), ele deve ter a qualificação de ineficácia no controle anterior até se encontrar em funcionamento e ser avaliada sua eficácia, momento no qual deverá ser revisada a avaliação dos riscos associados.

3.4.c **Saídas**

No final desta etapa, a avaliação inerente e residual dos riscos identificados deve ser realizada nos formulários definidos para esse fim, nos níveis VH (Very High - Muito Alto); H (High - Alto); M (Medium - Médio); L (Low - Baixo) e N (Null - Nulo), de acordo com a matriz RAM da empresa, e serem aprovados pelo proprietário do processo correspondente.

3.5 FASE 5 - IDENTIFICAÇÃO DE MITIGADORES ADICIONAIS E ALERTAS

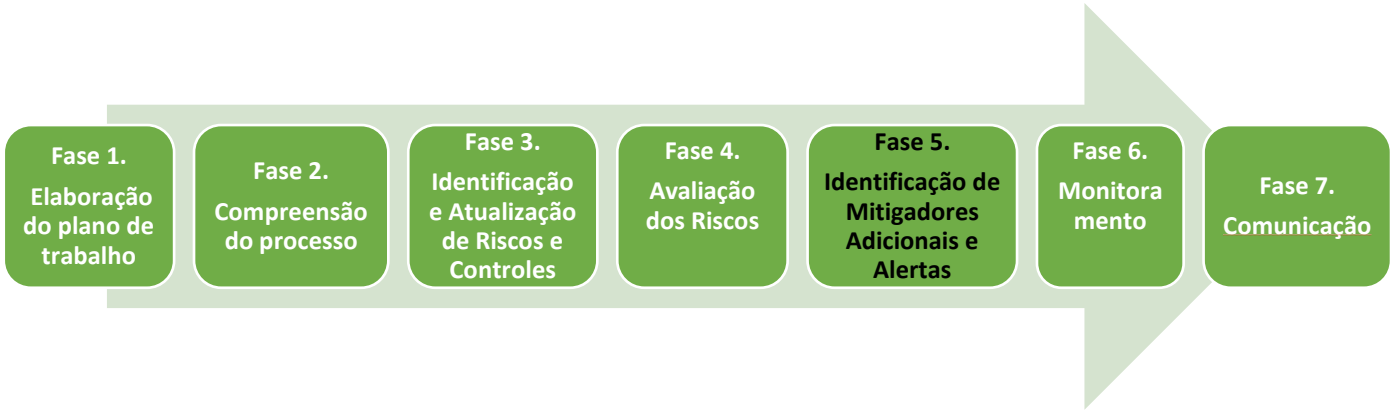
Esta etapa define as atividades adicionais de mitigação (controles ou ações de tratamento) que buscam prevenir as causas ou se proteger das consequências para aqueles riscos cujo valor residual seja "Muito alto", "Alto" e "Médio"[13], através da análise das causas identificadas e da eficácia de todos os mitigadores associados, de modo a selecionar a opção adequada entre as atividades de controle e as ações de tratamento economicamente viáveis para levar o risco residual a um valor de risco aceitável ("Baixo" ou "Nulo").

Se a avaliação do risco residual for "Médio", os mitigadores adicionais são opcionais e quem decide é o proprietário do processo, exceto para os seguintes casos:

- Quando os controles associados ao risco tiverem detectado falhas na concepção e na operacionalidade através de autoavaliações, testes da gerência, Revisão Fiscal ou monitoramentos preventivos no último ano.
- O risco seja da categoria estratégica.

Os alertas de risco ou KRI (Indicador Chave de Risco - Key Risk Indicator) são definidos como ferramentas de medição que permitem monitorar, de forma preventiva, o comportamento das variáveis associadas às causas dos riscos, para indicar mudanças no nível de exposição aos riscos, gerando alertas precoces que levam a reforçar ou focalizar a gerenciamento para evitar sua materialização. Os KRIs devem ser identificados para os riscos cuja avaliação residual tenha sido "Muito Alta" e "Alta" e com alinhamento direto com os objetivos estratégicos associados ao processo.

[13] De acordo com os níveis das matrizes de RAM de cada empresa.



3.5.a **Entradas**

- *Informações sobre riscos e medidas de mitigação*: Resultados do exercício de avaliação dos riscos, matriz de riscos e controles dos processos, matriz de riscos e controles transversais e de múltiplos executores[14], relatórios de auditorias internas ou externas realizadas no processo analisado, que podem ser um input para determinar novas medidas de mitigação, um relatório atualizado de eventos ocorridos, entre outros.

3.5.b **Processo[15]**

a. IDENTIFICAÇÃO DE NOVAS MEDIDAS DE MITIGAÇÃO

Deve ser estabelecida a medida de mitigação mais apropriada entre as atividades de controle e as ações de tratamento (AT) economicamente viáveis, de acordo com as seguintes opções:

- Atividades de Controle: Os controles são formulados ou redefinidos para mitigar as causas através de uma atividade sistemática e recorrente dentro do processo analisado.

- Ações de processamento: Se a causa do risco não puder ser controlada com uma atividade de controle recorrente, neste caso, deve ser criada uma ação de tratamento.

- Controles transversais: Se a causa pode ser mitigada através de uma atividade sistemática e recorrente a ser executada por todas as áreas da empresa, deve ser gerado o mitigador transversal com o processo de Governo.

[14] Se a Matriz de Risco e Controles estiver disponível, ela deve ser considerada durante o ano.
[15] As diretrizes para a construção de controles e ações de tratamento devem ser consultadas no "Procedimento para o gerenciamento de controlos e medidas de mitigação", GEE-P-006.

- Controles de múltiplos executores: Se a causa pode ser mitigada através de uma atividade sistemática e recorrente a ser executada por algumas áreas da empresa, o fator mitigador de múltiplos executores deve ser gerado em conjunto com o processo de Governo.

b. DEFINIÇÃO DE KRI[16]

Para a definição de alertas ou KRIs, você deve selecioná-los:

- As causas documentadas do risco com maior probabilidade de ocorrência[17].
- As causas que geraram a materialização do risco (quando aplicável)

Das causas selecionadas acima, escolha pelo menos uma e identifique quais variáveis podem ser objeto de medição e determine quais informações são necessárias para o desenho do indicador (como, quando e onde a informação da variável é obtida). Uma vez validada a disponibilidade da informação associada, formular uma KRI que cumpra os critérios definidos neste documento.

Note que um KRI:

- Deve ser específico e claro, mensurável (quantificável), baseado em informações disponíveis, recentes e confiáveis.

- Deve ter uma descrição clara ou intenção do que deve ser medido, considerando as exclusões ou limitações aplicáveis.

- A fórmula de cálculo do KRI deve conter a equação ou expressão matemática onde as variáveis e constantes utilizadas estão relacionadas, para obter o resultado.

- Deve ter um limite, que deve ser um valor numérico tolerável para a geração do alerta que indique o valor máximo (se sua tendência é negativa, indicando bom comportamento quando o resultado do KRI é inferior ao limite de alerta) ou um valor mínimo (se sua tendência é positiva, indicando bom comportamento quando o resultado do KRI é superior ao limite de alerta).

- Deve ter uma frequência de medição específica: semanal, mensal, trimestral. Para a definição desta frequência, devemos levar em conta o ciclo da informação ou dados de entrada, bem como a oportunidade na geração do alerta.

- Deve ser diferente dos indicadores de resultados dos objetivos do mapa estratégico da empresa e dos indicadores de processo, mas pode ser um indicador de meios, desde que esteja associado às causas selecionadas.

[16] Um exemplo de KRI pode ser encontrado nos anexos a este documento.

[17] Para determinar qual a causa com maior probabilidade de ocorrência, use o julgamento de especialistas.

3.5.c **Saídas**

No final desta fase você deveria ter:

- Medidas de mitigação novas ou atualizadas (Ações de Tratamento, Atividades de Controle, Controles Transversais, Controles de Múltiplos Executadores e Outros Fatores Mitigadores) e documentadas.
- KRIs desenhados.

3.6 FASE 6 - MONITORAMENTO DE RISCOS

O objetivo do monitoramento é verificar se os riscos identificados, avaliados e tratados estão permanentemente dentro dos limites toleráveis da empresa, de modo a fornecer feedback sobre o ciclo de risco e tomar medidas para garantir um gerenciamento adequado dos riscos.

O escopo do monitoramento de risco do processo inclui o acompanhamento das ações de tratamento, alertas gerados através de KRIs, as materializações de eventos e medição da eficácia dos controles e ações de tratamento através de auto avaliações, monitoramento preventivo do Controle Interno, Testes de Gerenciamento, auditorias internas e externas, entre outros.

3.6.a **Entradas**

- Matrizes de riscos e controles
- Resultados da avaliação.
- Alarmes de Risco - KRIs desenhadas
- Eventos materializados de riscos
- Informações sobre a execução de controles e ações de tratamento
- Informações sobre alterações externas que podem aumentar a exposição ao risco
- Resultados das Auto Avaliações de Controle Interno, Testes de Gerenciamento, Auditorias Internas e Externas.

3.6.b **Processo**

a. MONITORAMENTO DAS AÇÕES DE TRATAMENTO

Esta monitoramento[18] assegura um feedback sistemático sobre o progresso das ações de tratamento, fornecendo alertas face o planejado para gerir o risco e a medição da eficácia no final da sua execução.

Para acompanhar as ações de tratamento, o(s) implementador(es) da(s) ação(ões) de tratamento deve(m) relatar: (i) o progresso real da(s) ação(ões) de tratamento, que será um valor percentual de acordo com a conclusão das atividades do plano de trabalho e os marcos e datas definidas, (ii) comentários ou justificativas apoiando o estatuto de execução da ação, e (iii) medição da eficácia da ação no encerramento da ação.

O estatuto das ações de processamento deve ser atualizado periodicamente[19] e definido de acordo com o progresso real, o progresso planejado e a data de início e fim como detalhado a seguir:

- *Não iniciado*: A data de início não ocorreu e a ação não tem progresso associado.
- *Execução*: A data de início já ocorreu, a ação está no plano de trabalho estabelecido ou acima dele e a data de conclusão ainda não ocorreu.
- *Atraso*: A data de início já ocorreu e o progresso da ação não atingiu o nível planejado para o período ou a ação não tem progresso registrado ou a data final já ocorreu e a ação não foi concluída.
- *Fechado*: A data de conclusão já ocorreu e o progresso da ação é igual a 100%.
- *Cancelada*: A ação foi suspensa ou cancelada antes de atingir 100% de progresso.

A eficácia da implementação das ações de processamento deve ser gerida de acordo com as disposições do "Procedimento de Gerenciamento de Controles e Medidas de Mitigação", GEE-P-006. Se não for eficaz, deve-se entender que o risco não foi gerenciado e, portanto, o risco deve ser analisado novamente dentro do ciclo e seu impacto na avaliação do risco e a definição de mitigadores de risco e alertas deve ser considerada, conforme o caso.

b. MONITORAMENTO DE EVENTOS DE RISCO MATERIALIZADOS

Entende-se por eventos materializados a ocorrência de situações cujas consequências afetaram o cumprimento dos objetivos definidos para a estratégia, processos ou projetos. Para a análise dos eventos materializados, documentar pelo menos os seguintes elementos:

- Descreva em detalhes o evento materializado
- Data de ocorrência do evento
- Associar o evento a uma matriz de risco
- Determinar se a causa do evento foi identificada na matriz de risco e controle
- Estabelecer se o evento foi originado por pessoas, processos ou ambiente.

[18] Na Ecopetrol, o acompanhamento das ações de tratamento é feito pelo profissional da Gerência de Asseguramento de Controle interno mensal com base no que é reportado pelos processos.

[19] Na Ecopetrol, o acompanhamento ou revisão é feito mensalmente, reportando quando aplicável de acordo com o plano de trabalho/marcos definidos. Nas empresas é feito de acordo com o calendário ou periodicidade definida pela Gerenciamento Corporativa de Controle Interno da Ecopetrol.

- Determinar qual foi o impacto do evento em cada um dos recursos da empresa (por exemplo, pessoas, meio ambiente, economia, etc.)
- Identificar o agente mitigador estabelecido para a causa que originou o evento
- Analisar o projeto e operação de fatores de mitigação
- Defina a causa ou risco caso ele não tenha sido previamente identificada
- Estabelecer se o risco tem uma KRI definida associada à causa que o materializou
- Identificar se o KRI alertou sobre a possível materialização do evento
- Determinar se o evento ocorrido altera a avaliação de risco atual
- Estabelecer se o evento ocorrido envolve mudanças nos fatores de mitigação
- Documentar a ação a ser executada.

Com esta informação, valida-se a idoneidade da identificação dos riscos, causas e consequências; do mesmo modo, verifica-se a necessidade de ajustar os mitigadores existentes ou definir novas medidas, e valida-se e ajusta-se a avaliação dos riscos. Estes eventos e sua análise devem ser registrados no "Formulário de gerenciamento de materialização de riscos", GEE-F-044. Os planos de ação decorrentes da análise do evento materializado devem ser reportados pelos responsáveis pela sua execução e acompanhados pela Direção Corporativa de Asseguramento de[20]Controle Interno.

c. MONITORAMENTO DE ALERTAS GERADOS PELO KRI

Os KRIs podem alertar sobre alterações no nível de exposição e gerar alertas precoces que levam ao reforço ou foco do gerenciamento para evitar a sua materialização.

O relatório do KRI deve ser feito com a frequência estabelecida e em conformidade com as diretrizes de relatórios estabelecidas por cada empresa. As informações reportadas corresponderão a:

- O resultado do cálculo do KRI reportado pelo processo
- O estado de alerta ou não, de acordo com o resultado e os parâmetros de desenho definidos (por exemplo, unidade de medida, tendência e limite de alarme)
- A análise do motivo pelo qual o alerta foi gerado e a gerenciamento a ser realizada.

O monitoramento é gerido da seguinte forma:

- Quando o resultado de uma KRI estiver fora do seu limite de alerta, a Gerência Corporativa de Controle Interno deve rever a eficácia dos controles e as ações de tratamento associadas aos riscos; bem como avaliar a necessidade de ativar medidas de prevenção adicionais, implementar planos de ação alternativos ou focar o monitoramento em determinados fatores de risco, entre outros, de modo a minimizar as possibilidades de materialização dos eventos de risco.

- Fazer gráficos do comportamento dos resultados históricos que permitam visualizar se o KRI se afasta ou se aproxima do seu limite de alarme, para identificar tendências ou temporalidade nos resultados do KRI (ver anexos). Os gráficos são aplicados uma vez que existem dois ou mais relatórios KRI, para que uma tendência possa ser estabelecida.

[20] Na Ecopetrol, o acompanhamento ou revisão é feito mensalmente, reportando quando aplicável de acordo com o plano de trabalho/marcos definidos. Nas empresas é feito de acordo com o calendário ou periodicidade definida pelo Gerenciamento do Controle Interno Corporativo de Ecopetrol.

- Calcular a média e o número de vezes fora do limite durante o último ano de medições, de modo a analisar os resultados do KRI ao longo do tempo.

- Quando um evento se materializa, é importante analisar se existe um KRI associado à causa que gerou o evento e se este apresentou os respectivos alertas antecipados. Documentar esta análise no Formulário de Materialização de Risco. Se não foi emitido nenhum alerta, o desenho do KRI deve ser revisto e ajustado para refletir melhor as variáveis de risco.

d. ACOMPANHAMENTO DA EFICÁCIA DOS CONTROLES

As atividades de controle são acompanhadas pelo monitoramento de sua concepção e eficácia, o que é feito, pelo menos, através de:

- Auto-avaliações de Controle Interno
- Monitoramento Preventivo de Controle Interno
- Testes de Gerenciamento
- Auditorias Internas e Externas.

A eficácia da concepção e funcionamento dos controles deve ser gerida de acordo com o "Procedimento de Gerenciamento de Controles e Medidas de Mitigação", GEE-P-006.

3.6.c **Saídas**

O resultado da fase de monitoramento deve fornecer feedback sobre a identificação, avaliação e tratamento de riscos, dependendo das questões identificadas através de:

- Relatórios sobre o estado de execução das Ações de Tratamento
- Resultados dos KRIs
- Formulário com a análise de risco materializada
- Resultados das auto-avaliações de Controle Interno
- Relatórios de Monitoramento Preventivo de Controle Interno
- Observações do Teste de Gerenciamento
- Observações de auditoria interna e externa.

3.7 FASE 7 – COMUNICAÇÃO

A comunicação é definida como um processo interativo de troca de informações que permite a socialização de resultados, compartilhamento de dados, opiniões e perspectivas, facilitando o adequado fluxo de informações e o diálogo entre as partes interessadas ou envolvidas. A comunicação permite que cada etapa do ciclo de gerenciamento de risco seja construída em conjunto com as áreas e processos da

empresa.

A comunicação é implementada em cada uma das fases deste procedimento e deve garantir o seguinte:

- Geração de uma língua e cultura comum em relação ao gerenciamento de riscos.
- Feedback sobre o gerenciamento do risco através da incorporação dos resultados obtidos em cada uma das fases e da interação entre as áreas de execução do processo e a governança do Sistema de Controle Interno.
- Divulgação dos papéis e responsabilidades dos participantes e partes interessadas
- Divulgação de informações relevantes de gerenciamento de risco do processo.
- Identificação de sinergias entre as diferentes áreas para reforçar o gerenciamento do risco
- Incorporação do gerenciamento de risco como variável estratégica para a tomada de decisões

Para a comunicação do gerenciamento do risco do processo, está disponível o seguinte esquema:

Fase/ Elemento	Entregável	Periodicidade	Canal de comunicação/ Emissor	Receptor
Elaboração do plano de trabalho	Cronograma	Ecopetrol: Pelo menos anualmente Subsidiárias: De acordo com o guia GEE-G-002	E-mail do proprietário do processo/ Gerente de Conformidade da subsidiária	Gerência Corporativa de Asseguramento de Controle Interno
Identificação e atualização de Riscos e Controles	Matriz de risco e controles	Ecopetrol: Mensal Subsidiárias: De acordo com o guia GEE-G-002	Ecopetrol: BWise Subsidiárias: Relatório de Gerenciamento de Riscos	Gerência Corporativa de Asseguramento de Controle Interno
Avaliação de Riscos	Formulário de avaliação de risco.	Ecopetrol: mínimo anual ou quando necessário Subsidiárias: De acordo com o guia GEE-G-002	E-mail do dono do processo/ Gerente de Conformidade da subsidiária	Gerência Corporativa de Asseguramento de Controle Interno

Identificação de Mitigadores e alertas adicionais de risco	Matriz de risco e controles	Ecopetrol: Mensal Subsidiárias: De acordo com o guia GEE-G-002	Ecopetrol: BWise Subsidiária: Relatório de Gerenciamento de Riscos	Gerência Corporativa de Asseguramento de Controle Interno
Os eventos de risco materializados	Formulário de materialização do risco GEE-F-044	Ecopetrol: Cada vez que um evento acontece Subsidiárias: De acordo com o guia GEE-G-002	E-mail do dono do processo onde o evento foi detectado/ Gerente de Conformidade da subsidiária	Gerência Corporativa de Asseguramento de Controle Interno
Ações de Tratamento	Relatório de acompanhamento/eficácia Bwise para a Ecopetrol Matriz de risco e controle	Ecopetrol: Mensal E cada vez que uma parte de tratamento Subsidiárias: De acordo com o guia GEE-G-002	Ecopetrol: Bwise / Executor da ação de tratamento Subsidiária: Relatório de Gerenciamento de Riscos	Gerência Corporativa de Asseguramento de Controle Interno
Controles	Relatórios de: auto avaliações, testes de gerenciamento, monitoramento preventivo, auditorias internas e externas	Auto avaliações Trimestralmente Testes de gerenciamento, monitoramento preventivo, auditorias internas e externas, na realização de avaliações de controle	Auto-avaliações: Ecopetrol: Bwise Subsidiárias: auto-avaliações Outros monitores: Ecopetrol: Relatórios de monitoramento Subsidiárias: Formulário dos resultados de acordo com a periodicidade definida	Gerência Corporativa de Asseguramento de Controle Interno
KRIs	Ecopetrol: Relatório BWise Subordinado: Matriz de risco e	Ecopetrol: Mensal Subsidiárias: De acordo com o guia GEE-G-002	Ecopetrol: BWise Subsidiárias: Formulário de Gerenciamento de Riscos	Gerência Corporativa de Asseguramento de Controle Interno

4. CONTINGÊNCIAS

Não se aplica.

LISTA DE VERSÕES

Documento Anterior			
Versão	**Data dd/mm/aaa**	**Código e título do Documento**	**Alterações**

Novo Documento		
Versão	**Data dd/mm/aaa**	**Alterações**
1	31/01/2018	Revogação: PDO-P-025 Procedimento do Ciclo de Risco PDO-I-027 Instruções para o desenho e acompanhamento das Ações de Tratamento PDO-G-039 Guia para o Desenho, Teste e Implementação de KRIs PDO-I-017 Instruções sobre Construção e Atualização de Matrizes Integrais de Controle Interno PDO-I-030 Instrutor de Avaliação de Riscos.
2	05/02/2019	Inclusão da análise de transações e contas significativas Inclusão da categorização de riscos. Revoga o formulário GEE-F-045. Atualização do capítulo sobre avaliação de risco Nota: É publicado com esta data uma vez que esta é a data de divulgação do documento, que foi utilizado para efeitos de execução do ciclo de gerenciamento de risco do termo.

Para mais informações, por favor entre contate com:

Autor(es): Edna Carolina Vargas
Telefone: 50559 **E-mail:** geraseconint@ecopetrol.com.co
Unidade: Gerência Corporativa de Asseguramento de Controle Interno

Revisado eletronicamente por:	**Aprovado eletronicamente por:**
ANGÉLICA MARIA ALAIX M **Profissional** **Cartão de Cidadania n. º 52.516.825** **Gerência Corporativa de Asseguramento de Controle Interno** **MÓNICA JIMÉNEZ G.** **Secretária Geral** **Cartão de Cidadania n. º 52.411.766** **Secretária Geral & Suporte à Presidência**	**HELBER ALONSO MELO HERNÉNDEZ** **Gerente Corporativo de Asseguramento de Controle Interno** **Cartão de Cidadania n. º 79.862.626** **Gerência Corporativa de Asseguramento de Controle Interno**

5. ANEXO 1

Exemplo de um KRI

Objetivo	Risco	Porqu	KRI
Assegurar o início, execução, encerramento e balanço dos contratos	Incumprimento das obrigações acordadas no contrato	Não tomar medidas atempadas sobre alertas, pedidos, pagamentos, reclamações de monitoramento de contratos feito pelo empreiteiro.	Percentagem de contratos com reclamações por supostas não conformidades da Ecopetrol

Descrição: Percentagem de contratos com reclamações pela suposta não conformidade da Ecopetrol. Este KRI monitora a causa: Não tomar medidas oportunas sobre alertas de acompanhamento de contratos, pedidos, pagamentos, reclamações feitas pelo empreiteiro.

Fórmula: Número de contratos com reclamações pela suposta não conformidade da Ecopetrol no mês / Número de contratos em andamento e em fechamento e balanço.

Frequência de medição: Mensal

Unidade de medida: Porcentagem

Fonte: - Relatório nacional consolidado, aba de reclamações do mês.
- Relatório de contratação SAP oficial TODAS AS EMPRESAS

Limite de alerta: 0,15% (valor máximo)

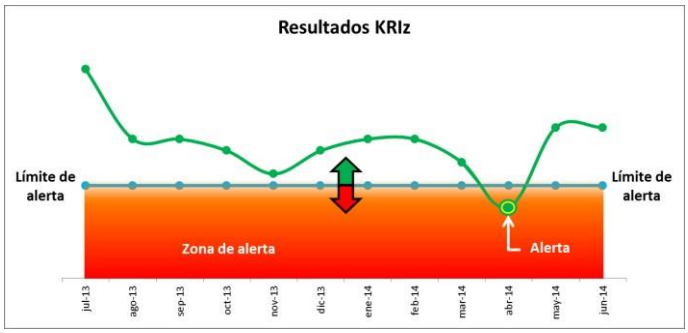
Tendência: Negativo (valores abaixo do limite de controle indicam melhor comportamento)

Localização da Evidência: Arquivo de medição dos EAU localizado no SharePoint da Gerência de Suprimentos.

6. ANEXO 2

Exemplo de Tendência KRIS

Exemplo de resultados de KRI com limite de alerta máximo (tendência negativa).



Exemplo de resultados de KRI com limite de alerta mínimo
(tendência positiva).

7. ANEXO 3

De modo a incorporar explicitamente o evento de risco de conformidade que contempla as questões de fraude, corrupção, suborno, lavagem de dinheiro e financiamento do terrorismo, e violações da lei FCPA nas matrizes de riscos e controles de seus processos, a seguir colocamos um evento genérico que deve ser incorporado para cada processo com as respectivas causas e consequências, de acordo com seu contexto e particularidades de acordo com o nível de implantação da matriz de risco e controle.

EVENTO DE RISCO DE CONFORMIDADE GENÉRICO: *Eventos de fraude, corrupção, suborno, branqueamento de capitais, financiamento do terrorismo e violações da Lei FCPA no processo "Nome do Processo/Sub-Processo".*

A identificação desses eventos deve ser realizada durante a fase 3 do ciclo de *identificação e atualização dos riscos e controles* do ciclo de gerenciamento dos riscos do processo, e as fases restantes do ciclo devem ser realizadas sobre os eventos identificados, garantindo assim o desenho particular de cada um desses riscos, de acordo com a natureza dos processos.

A seguir, propõe-se um risco como exemplo:

Processo nível 1	Descrição do objetivo do processo	Nome do risco	Descrição do risco
Gerenciamento de Contratos	Assegurar o início, execução, encerramento e balanço dos contratos, executando um gerenciamento adequada de eventualidades e avaliando o desempenho do empreiteiro.	Eventos de fraude, corrupção, suborno, branqueamento de capitais, financiamento do terrorismo e violações da lei FCPA no processo de Gerenciamento de Contratos	Eventos de fraude, corrupção, suborno, branqueamento de capitais, financiamento do terrorismo e violações da lei FCPA no processo de Gerenciamento de Contratos. Por causa de: - Receber ou autorizar pagamentos por bens e/ou serviços que não cumpram as condições acordadas, ou que não tenham sido recebidos. - Modificação de informações contratuais nos sistemas por parceiros não autorizados - Mau uso de recursos na execução do contrato. - Pagamentos em duplicado. - Vazamento de informações críticas do processo. Isto pode levar a processos judiciais e perdas económicas.