

GUIA PRÁTICO DA METODOLOGIA DE GERENCIAMENTO DE RISCOS DA CODEVASF



Por que gerenciar riscos?

“Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público.”*

“Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos.”*

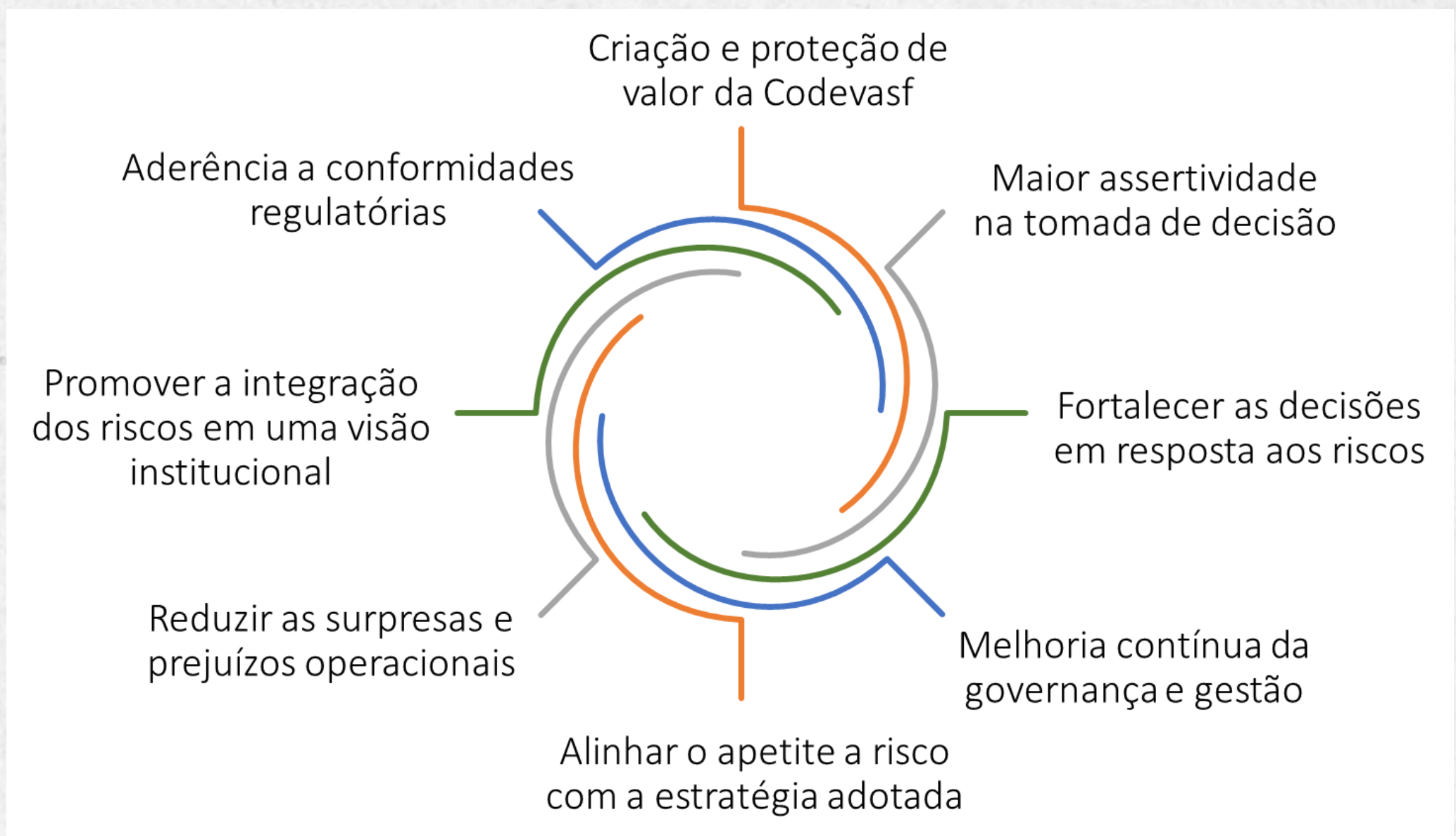


Figura 1. Objetivos do Gerenciamento de Riscos na Codevasf.

Metodologia



Figura 2. Interação das etapas metodológicas com os instrumentos de planejamento, insumos a produtos definidos.

Entendimento do contexto

Etapa 1

- Identificação e priorização dos processos de trabalho e iniciativas.
- Estabelecimento dos Objetivos, Escopo e Contexto.
- Conhecimento do Negócio (Diagramação).

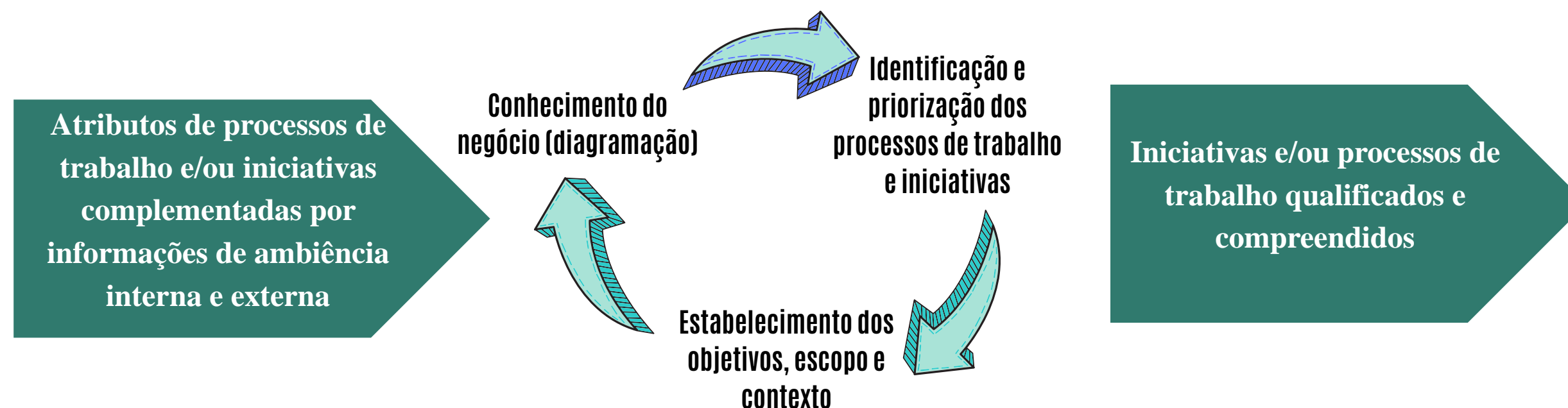


Figura 3. Entradas e saídas estabelecidas para a etapa de “Entendimento do Contexto”.

Entendimento do contexto

Etapa 1



Identificação e priorização dos processos de trabalho e iniciativas.

Nesta etapa, são identificados e caracterizados os processos de trabalho da unidade orgânica, alinhados aos macroprocessos e à missão institucional. A priorização é feita por meio da **Avaliação de Impacto no Negócio (BIA)**, que analisa o efeito da interrupção total de cada processo com base nos seguintes critérios:

- **Tempo máximo tolerado** de interrupção;
- **Impacto operacional** – afeta diretamente as operações;
- **Impacto legal** – descumprimento de leis, normas ou regulamentos;
- **Impacto na imagem** – dano reputacional perante órgãos de controle, sociedade e mídia;
- **Impacto financeiro** – multas, prejuízos e perdas de receitas.

Ao final, os processos são classificados como **essenciais**, **relevantes** ou **moderados**. Apenas os processos essenciais e relevantes seguem para as etapas de análise de riscos no ciclo vigente.

Entendimento do contexto

Etapa 1

➤ Conhecimento do Negócio (Diagramação).

Na diagramação dos processos de trabalho que integram os processos organizacionais da unidade orgânica objeto do gerenciamento de riscos, deverá ser empregada a metodologia de modelagem funcional *Integrated Definition Methods - IDEF*, mantida e desenvolvida pelo *Computer Systems Laboratory of the National Institute of Standards and Technology – NIST*.

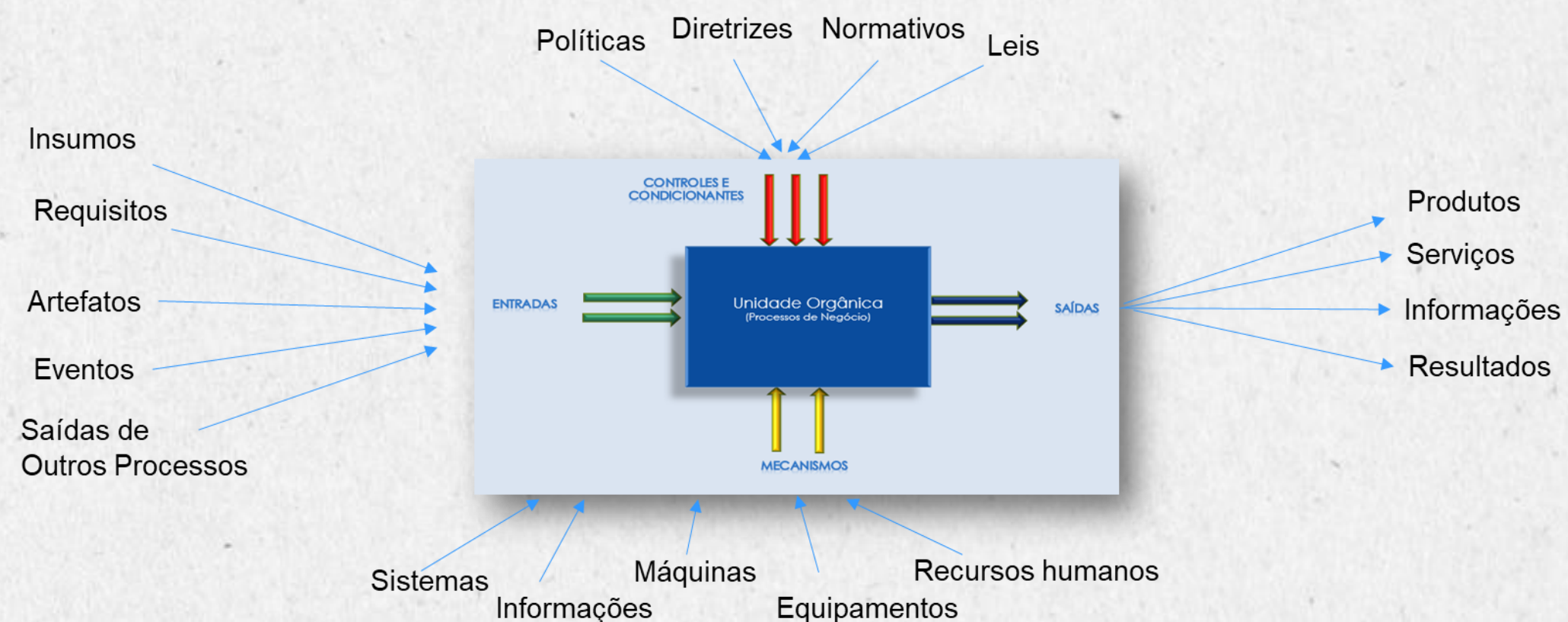


Figura 4. Exemplo de Diagramação

Entendimento do contexto

Etapa 1



Compreender quais fatores influenciam o atingimento dos seus objetivos e em qual contexto se insere, no interno ou externo à organização.



Formas de entendimento de contexto



Analisar documentos e informações específicas do empreendimento;



Analisar dados históricos de projetos similares; e



Conhecimento acumulado a partir de empreendimentos semelhantes.



Essa análise pode ser complementada por meio de técnicas que facilitam a identificação destes e demais riscos, como: *brainstorming*, entrevista e análise de premissas do empreendimento

Ambiente Interno

STRENGTH
(FORÇAS)

S

W

WEAKNESS
(FRAQUEZAS)

OPPORTUNITIES
(OPORTUNIDADES)

O

T

THREAT
(AMEAÇAS)

Ambiente Externo

Figura 5. Análise SWOT

Identificação dos Riscos

Etapa 2

2.1 Identificação dos Fatores de Risco

➤ Riscos possíveis e aplicáveis que podem dar causa aos eventos de risco.

➤ Originados por questões envolvendo pessoas, processos, sistemas, tecnologia, infraestrutura e fatores externos.

Identificação dos
Eventos de Risco

Identificação dos
Fatores de Risco

2.2 Identificação dos Eventos de Risco

➤ Eventos que podem impedir ou prejudicar o atingimento dos objetivos idealizados para os processos de trabalho, ou ainda as metas estabelecidas sejam alcançadas.

Figura 6. Atividades integrantes da etapa de Identificação dos Riscos.

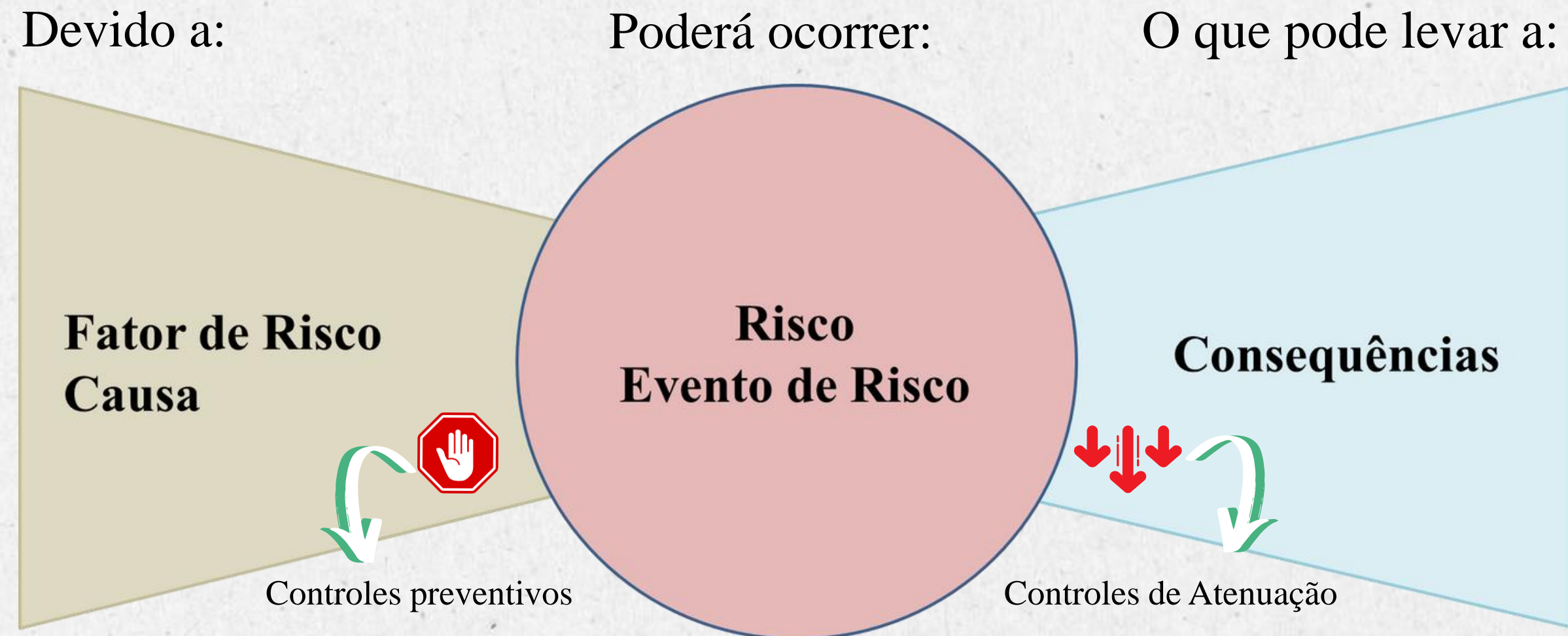


O evento de risco não pode ser confundido com o que lhe dê causa ou com um problema do dia a dia.

O que é risco?



O efeito da incerteza sobre os objetivos.



Técnica "Bow Tie"

Figura 7. Técnica Bow Tie.

Análise e Avaliação dos Riscos

Etapa 3

3.1 Análise de Riscos

3.2 Avaliação de Riscos

Técnica “Bow Tie”

Probabilidade de ocorrência dos eventos de risco e o impacto resultante, mediante avaliação qualitativa.



Impacto					
Critérios de Avaliação					
Manutenção dos Projetos, Processos e/ou Ações (MP)	Regulação e Controle (RC)	Imagem da Codevasf (IMG)	Missão Institucional (MI)	Intervenção de Gestão para Atenuação do Impacto (IG)	Orçamentário/ Financeiro (OF)
Potencial impacto em caso de materialização dos riscos nos Projetos, Processos e/ou Ações da Empresa, considerando a dificuldade de normalização.	Impacto da interferência de Órgãos de Regulação ou de Controle Interno e Externo nas Projetos, Processos e/ou Ações da Codevasf.	Potencial dano à imagem da empresa e à sua reputação.	Potencial prejuízo à missão institucional da Codevasf.	Nível de intervenção da gestão para resolução do problema em caso de materialização do risco.	Impacto orçamentários-financeiro resultante da materialização do risco.

Figura 8. Critérios de avaliação de impacto

Probabilidade (Critérios para análise)					
Critérios	Evento <u>pode</u> ocorrer apenas em circunstâncias excepcionais	Evento <u>pode</u> ocorrer em algum momento	Evento <u>deve</u> ocorrer em algum momento	Evento <u>provavelmente</u> ocorra <u>na maioria</u> das circunstâncias	Evento <u>esperado</u> que ocorra <u>na maioria</u> das circunstâncias
Frequência Observada / Esperada	Muito baixa (< 10%)	Baixa (>=10% <=30%)	Média (>30% <=50%)	Alta (>50% <= 90%)	Muito alta (>90%)
Peso	1	2	3	4	5

Figura 9. Critérios para avaliação da probabilidade

3.3 Avaliação da Criticidade de Riscos – Impacto x Probabilidade

		Matriz de Riscos (Inerente e Residual)					
IMPACTO	Muito Alto	5					
	Alto	4					
	Moderado	3					
	Pequeno	2					
	Insignificante	1					
			1	2	3	4	5
		Muito Baixa	Baixa	Média	Alta	Muito Alta	
		< 10%	>=10% <=30%	>=30% <= 50%	>=50% <= 90%	>90%	
PROBABILIDADE							
Nível de Risco							
Níveis							
RE - Risco Extremo							
RA - Risco Alto							
RM - Risco Moderado							
RB - Risco Baixo							

➤ O nível de risco inerente será obtido a partir da multiplicação da probabilidade e do impacto decorrente, sem considerar a existência de qualquer controle operacional.

$$NRI = P \times I$$

NRI: Nível de Risco Inerente
P: Probabilidade de ocorrência
I: Impacto

Figura 10. Matriz de criticidade de riscos inerentes e residuais.

3.3 Avaliação da Criticidade de Riscos - Controles

Avaliação dos Controles	
Eficiência da Atuação	Considerações
Inexistente	Os controles são inexistentes ou sem efetividade para o propósito segundo o qual foram desenhados.
Fraco	Os controles não cumprem com seu propósito na forma idealizada ou são empregados segundo critérios individuais sem qualquer padronização de procedimentos.
Mediano	Os controles implementados mitigam parcialmente o nível de risco, face a deficiência em seu desenho, escopo de atuação limitado ou emprego de técnicas e ferramentas inadequadas.
Satisfatório	Os controles implementados são satisfatórios em mitigar o nível de risco, mas oferecem oportunidades de aperfeiçoamento nas ferramentas empregadas, nos procedimentos adotados ou no envolvimento de atores.
Forte	Os controles implementados podem ser considerados bastante eficientes em mitigar o nível de risco, empregando ferramentas e procedimentos corretos e envolvendo os atores requeridos.



A partir da avaliação de eficiência dos controles existentes em mitigar o nível de risco inerente, calcula-se então o nível de risco residual (riscos remanescentes após aplicação dos controles):

$$NRR = NRI \times GI$$

NRR: Nível de Risco Residual
NRI: Nível de Risco Inerente
GI: Grau de Ineficiência do Controle

Figura 11. Avaliação do grau de eficiência dos controles empregados.

Apetite ao risco

Em Processos

- Moderado e tem como escopo todas as unidades orgânicas da Codevasf;
- Todos os riscos altos e extremos serão obrigatoriamente tratados, podendo os baixos e moderados serem aceitos e monitorados ao longo do tempo.



Apetite ao risco: nível de risco que a Codevasf está disposta a aceitar.

Nível de Risco	Possíveis Respostas ao Risco
Risco Extremo	Evitar: Não iniciar, ou descontinuar as atividades que geram o risco. Ex. Suspender um produto em uma determinada região, não executar um determinado projeto etc. Excepcionalmente podem ser empregados controles para mitigar o risco à faixa de apetite ao risco de forma justificada e quando o custo/benefício assim o permitir. Transferir/Compartilhar/Mitigar: Transferir ou compartilhar todo ou parte do risco, reduzindo a probabilidade e/ou seu impacto ou adotar medidas para reduzir a probabilidade e/ou impacto dos riscos mediante aperfeiçoamento de controles preventivos e de atenuação existentes e/ou adoção de novos controles.
Risco Alto	Transferir/Compartilhar/Mitigar: Transferir ou compartilhar todo ou parte do risco, reduzindo a probabilidade e/ou seu impacto ou adotar medidas para reduzir a probabilidade e/ou impacto dos riscos mediante aperfeiçoamento de controles preventivos e de atenuação existentes e/ou adoção de novos controles.
Risco Moderado	Aceitar: Conviver com o evento de risco mantendo práticas, procedimentos e controles existentes, ou ainda avaliando a possibilidade de retirar controles mantendo o apetite ao risco.
Risco Baixo	Aceitar: Conviver com o evento de risco mantendo práticas, procedimentos e controles existentes, ou ainda avaliando a possibilidade de retirar controles mantendo o apetite ao risco.



O Apetite será variável conforme a disciplina e deve ser aprovado pela alta gestão.

Figura 12. Apetite ao Risco em Processos

Tratamento e Resposta ao Risco

Etapa 4

4.1 Estabelecimento do tipo e medidas de tratamento

Medidas de Tratamento	
Nada a Fazer	Os riscos serão aceitos e nada será feito, uma vez que eles estão dentro do apetite ao risco definido
Retirar Controles	Os controles existentes são demasiadamente eficientes e um ou outro poderá ser retirado sem compromisso do nível de risco aceitável segundo o apetite ao risco definido.
Manter Controles	Os controles existentes são suficientemente eficientes em manter o nível de risco dentro do apetite ao risco definido
Implantar Controles	Será preciso desenhar e implantar novos controles para manter o nível de risco dentro do apetite ao risco
Aperfeiçoar Controles	Os controles existentes serão aperfeiçoados para que sua eficiência mantenha o nível de risco dentro do apetite ao risco definido
Aperfeiçoar/Implantar Controles	Serão tomadas medidas para aperfeiçoar controles existentes e ainda desenhar e implantar novos para manter o nível de risco dentro do apetite ao risco definido



Tipo de Tratamento do Risco	
Tipo	Ação a Realizar
Aceitar	Nada a fazer
Mitigar	Aperfeiçoar controles existentes e/ou implantar novos para mitigar riscos
Compartilhar	Compartilhar os riscos com terceiros de forma a minimizar prejuízos
Transferir	Repassar o risco a terceiros de forma a não sofrer os prejuízos resultantes da materialização do evento de risco
Evitar	Desistir de empregar o ativo de negócio (processo ou iniciativa) de forma a não sofrer risco

4.2 Formulação do plano de tratamento

Consiste em registrar, para cada evento de risco associado, uma medida de tratamento, os controles preventivos e de atenuação que serão objeto de implantação ou aperfeiçoamento, bem como informações complementares relativas à sua implementação.



4.3 Implementação do plano de tratamento

Implementar as iniciativas previstas na atividade anterior visando a retirada, aperfeiçoamento ou implementação dos controles.



Os indicadores dessa fase deverão:

- ser mensuráveis;
- ser previsíveis;
- ser comparáveis segundo diferentes ciclos ou períodos de avaliação;
- ter um responsável designado; e
- contemplar o contexto do negócio.

Monitoramento e Análise Crítica

- Constitui suporte a todas as etapas do gerenciamento de riscos;
- Monitorar situações de mudanças;
- Deve ser praticado após conclusão da implantação dos controles previstos e durante os ciclos de gerenciamento de riscos, periodicamente.



Comunicação e Consulta

- Processo de suporte preconizado na norma ABNT ISO 31.000:2018;
- A “Comunicação” deve promover conscientização e entendimento e a “Consulta”, maximizar a obtenção de retorno e informação auxiliando o processo de tomada de decisão.

- **A Análise Crítica deverá conter, no mínimo:**
 - Inserção de novos riscos, sua análise, avaliação e tratamento ou a retirada de riscos identificados em ciclo anterior que não se justifiquem mais;
 - Avaliação dos controles implantados, mediante aferição das metas estabelecidas para seus indicadores de desempenho;
 - Relatos de incidentes que materializaram riscos sob controle, para levantamento das razões que lhe deram causa e propostas de ações corretivas;
 - Fatores motivadores que requeiram alteração do tipo ou da medida de tratamento na resposta a riscos identificados em ciclos anteriores;
 - Retirada de controles existentes ou implantação de novos controles face a alteração do nível de criticidade dos riscos associados.

**Secretaria de Riscos e Controle Interno
– PR/SRC –**

Telefones: 61 2028-4354 ou 61 2028-4564

E-mail: pr.src@codevasf.gov.br

Acesse o material:

<https://educa.codevasf.gov.br/>

[MGR - Metodologia de Gerenciamentos de Riscos da Codevasf](#)