Gestão de Riscos

Rodrigo Fontenelle de A. Miranda, CGAP, CRMA, CCSA

Agenda

- Instrução Normativa Conjunta MP / CGU nº 01/2016
- Gestão de Riscos e Controles Internos
- Integridade, Riscos e Controles no MP

Controles internos, Gestão de Riscos e Governança no âmbito do Poder Executivo Federal

IN MP/CGU Nº 01/2016

Contextualização

Alinhamento Externo

Fortalecer a Gestão Estratégica, por meio da geração de informações e indicadores de risco, assegurando a aderência regulatória e o auxilio à tomada de decisão, base para a governança eficaz

Responder às sinalizações dos órgãos de controle quanto à necessidade da melhoria da gestão de riscos na governança do Setor Público, com a incorporação de boas práticas, privilegiando ações preventivas

IN Conjunta MP/CGU Nº 01, DE 10/05/2016

Dispõe sobre....

- Conceitos
- Controles Internos da Gestão
- Gestão de Riscos
- Governança
- Comitê de Governança, Riscos e Controles
- Disposições Finais

Para garantir a MISSÃO INSTITUCIONAL...

... São definidos OBJETIVOS ESTRATÉGICOS.

Para atingi-los, implementamos a GESTÃO DE RISCOS.

Como resposta aos riscos avaliados, elaboramos CONTROLES INTERNOS.

Para avaliar esses controles internos de forma independente, temos a AUDITORIA INTERNA.

Controles Internos

Os órgãos e entidades do Poder Executivo Federal deverão:

Implementar, manter, monitorar e revisar os controles internos da gestão

1ª Linha (ou camada) de defesa das organizações públicas

Ter por base a identificação, a avaliação e o gerenciamento de riscos

Considerar os riscos que se pretende mitigar tendo em vista os objetivos das organizações públicas

Ter controles adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto nos objetivos organizacionais

Os controles serão operados por todos os agentes públicos responsáveis por macroprocessos finalísticos e de apoio

Controles Internos

Os controles internos da gestão devem:

- Ser efetivos e consistentes de acordo com a natureza, complexidade, estrutura e missão do órgão ou da entidade pública
- Considerar os seguintes componentes: **ambiente de controle**, **avaliação de riscos**, **atividade de controle**, **informação e comunicação**, e **monitoramento**
- Basear-se no gerenciamento de riscos
- Integrar as atividades, planos, ações, políticas, sistemas, recursos e esforços de todos que trabalhem na organização
- Ser implementados como uma série de ações que permeiam as atividades da organização

Os componentes aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública

Gestão de Riscos

Instituir, em até 12 meses, **Política de Gestão de Riscos**, especificando ao menos:

- princípios e objetivos organizacionais
- diretrizes
- competências e responsabilidades

Os órgãos e entidades do Poder Executivo federal deverão:

implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e objetivos estratégico, observando:

- Princípios da Gestão de Riscos
- Objetivos da Gestão de Riscos
- Estrutura do Modelo de Gestão de Riscos
- Responsabilidades

Comitê de Governança, Riscos e Controles

Instituir nos órgãos e entidades do Poder Executivo Federal:

(maio/2017)

Apoiado pelo Assessor Especial de Controle Interno

Composto pelo dirigente máximo e pelos dirigentes das unidades a ele diretamente subordinadas

Comitê de Governança, Riscos e Controles Internos

Disposições Finais

A CGU poderá avaliar:

- A **Política** de Gestão de Riscos

- Se os **procedimentos de riscos** estão de acordo com a Política de Gestão de Riscos

- Os **controles internos** da gestão implementados pelos órgãos e entidades para mitigar os riscos, bem como outras respostas aos riscos avaliados

COSO II – *Committe of Sponsoring Organizations of The Treadway Commission*

Gerenciamento de Riscos Corporativos – Estrutura Integrada

Ministério do Planejamento, Desenvolvimento e Gestão - MP

Agenda

- Objetivos da Gestão de Riscos no Poder Executivo Federal
- Falando de Riscos
- Planejamento Estratégico Seges
- COSO II - Gerenciamento de Riscos Corporativos
- Atributos desejáveis para Gerenciar Riscos
- Desafios

Objetivos da Gestão de Riscos no Poder Executivo Federal

Assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham **acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização**, inclusive para determinar questões relativas à delegação, se for o caso

Aumentar a probabilidade de **alcance dos objetivos da organização**, reduzindo os riscos a níveis aceitáveis

Agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização

Fonte: Art. 15, IN Conjunta MP/CGU Nº 01/2016, de 10 de maio de 2016.

RISCO

Exemplo cotidiano

Objetivo: chegar ao trabalho até às 09:00

Casa	Metrô 25 min	Caminhada 10 min	Trabalho 09:00

Exemplo cotidiano

Incertezas:

1. Vai acordar no horário?
2. O metrô vai passar no horário?
3. A viagem vai durar realmente 25 minutos?
4. Vai conseguir fazer a caminhada em 10 minutos?

Exemplo cotidiano

Eventos:

1. Acordar tarde devido ao alarme não funcionar.
2. Greve do metrô, fazendo com que os trens atrasem.
3. Problemas no freio fazem com que o trem ande mais devagar, por segurança.
4. Algumas ruas estão fechadas devido a uma manifestação.

Exemplo cotidiano

Consequência

1. Não estar pronto para sair de casa no horário previsto.
2. Não vai conseguir sair da estação no horário previsto.
3. Não vai conseguir chegar no destino no horário previsto.
4. Levará mais tempo para chegar no trabalho.

Risco

Objetivo

Efeitos

Incertezas

Gestão de Riscos – Benefícios (Orange Book, 2004)

Uma boa gestão de riscos permite à organização:

Aumentar a confiança em alcançar os resultados desejados

Reduzir as ameaças para níveis aceitáveis de maneira efetiva

Tomar decisões para explorar oportunidades de maneira adequada

Planejamento Estratégico do MP e Gestão de Riscos

- ✓ **Instrução Normativa** Conjunta MP/CGU nº **001**, de 10 de maio de 2016.

- ✓ Programa de Integridade, instituído pela **Portaria GM/MP nº 150,** de 4 de maio de 2016, que tem a finalidade de mitigar ocorrências de desvios éticos, a partir da mobilização e participação ativa dos gestores públicos.

- ✓ A eficaz implementação dessas ferramentas requer que todos os níveis da organização tenham objetivos claros, fixados e comunicados. A explicitação de **objetivos, alinhados à missão e à visão do Ministério**, é necessária para permitir a identificação de eventos que potencialmente impeçam a consecução desses objetivos.

Planejamento Estratégico do MP

(SHANFIELD; HELMING, 2008)

Planejamento Estratégico do MP - Seges

1 - Modernizar a gestão pública, priorizando a inovação e a melhoria dos processos

- Inovar, simplificar e melhorar processos e serviços públicos
- **Aprimorar a gestão e elevar a efetividade e a transparência das transferências voluntárias**
- Aperfeiçoar as estruturas organizacionais e profissionalizar a ocupação dos cargos e funções que as compõem
- Implementar modelo de gestão estratégica de pessoas voltada a quadros de alto nível na APF

3 - Aprimorar a gestão do gasto público, com foco na qualidade

- Aprimorar os processos de aquisição de bens e serviços no Poder Executivo federal

COSO II - Processo de Gerenciamento de Riscos

A obra Gerenciamento de Riscos Corporativos – Estrutura Integrada, **amplia o alcance dos controles internos** do COSO I (publicado em 1992 e atualizado em 2013), oferecendo um **enfoque mais vigoroso e extensivo ao tema**, com ênfase no gerenciamento de riscos corporativos.

A estrutura de gerenciamento de riscos corporativos, embora não tenha por meta substituir a estrutura de controles internos das organizações, **incorpora estrutura de controle interno em seu conteúdo** e poderá ser utilizada, tanto para **atender às necessidades de controle interno** quanto para **adotar um processo completo de gerenciamento de riscos.**

Fonte: COSO II

COSO II - Gerenciamento de Riscos Corporativos

Estrutura Integrada:

O gerenciamento de riscos corporativos é um **processo conduzido em uma organização** pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para **identificar** em toda a organização **eventos em potencial**, capazes de afetá-la, e **administrar os riscos** de modo a mantê-los compatíveis com o **apetite a risco** da organização e possibilitar **garantia razoável** do cumprimento dos seus objetivos.

COSO II - Gerenciamento de Riscos Corporativos

Missão do MP:

- ✓ Promover o desenvolvimento, a gestão eficiente, a melhoria do gasto público e a ampliação dos investimentos, visando à oferta de bens e serviços de qualidade ao cidadão.

Objetivos Estratégicos MP:

- ✓ Modernizar a gestão pública, priorizando a inovação e a melhoria dos processos

Objetivos Estratégicos Seges (de contribuição da unidade):

- ✓ Aprimorar a gestão e elevar a efetividade e a transparência das transferências voluntárias

COSO II - Gerenciamento de Riscos Corporativos

No COSO II:

Os componentes passaram de 5 para 8

1. Ambiente Interno
2. **Fixação de Objetivos**
3. **Identificação de Eventos**
4. Avaliação de Riscos
5. **Resposta a Riscos**
6. Atividades de Controle
7. Informações e Comunicações
8. Monitoramento

As categorias de objetivos passaram de 3 para 4

COSO II – Categorias de Objetivos

Na estrutura de gerenciamento de riscos corporativos, orientada a fim de alcançar os objetivos de uma organização, foi inserida mais uma categoria, a estratégica.

Dessa forma, no COSO II as **4 categorias** são:

- ✓ **Estratégicos:** objetivos e metas alinhados à missão da entidade
- ✓ **Operacionais:** utilização eficaz e eficiente dos recursos
- ✓ **Comunicação:** confiabilidade dos relatórios
- ✓ **Conformidade:** cumprimento das leis e regulamentos aplicáveis

COSO II – 1º Componente: Ambiente Interno

Filosofia de gerenciamento de riscos	Atribuição de autoridade e de responsabilidade
Apetite a risco	Integridade e valores éticos
Comprometimento da alta administração	Compromisso com a competência

O ambiente interno compreende o **tom de uma organização e fornece a base pela qual os riscos são identificados e abordados.**

COSO II – 1º Componente: Ambiente Interno

Princípios[1]

- Compromisso perante valores éticos e de integridade
- Exercício de responsabilidade pela supervisão
- Definição da estrutura, autoridade e responsabilidade
- Compromisso com a competência
- Atribuição de responsabilidades

[1] COSO 2013

COSO II – 2º Componente: Fixação dos Objetivos

Definidos pela alta administração, devem ser divulgados a todos os componentes da organização, **antes da identificação dos eventos** que possam influenciar na consecução dos objetivos.

Os objetivos devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

- ✓ **Objetivos Estratégicos**
- ✓ **Objetivos Correlatos (operacional, comunicação e conformidade)**
- ✓ **Apetite e Tolerância a risco**

É uma precondição à identificação de eventos, à avaliação de riscos e às respostas a esses riscos.

COSO II – 2º Componente: Fixação dos Objetivos

Objetivos Estratégicos: relacionado à sobrevivência, continuidade e sustentabilidade. Metas de alto-nível, alinhadas à missão e visão da organização.

Objetivos Correlatos

- **operacional -** efetividade e eficiência na utilização dos recursos, mediante operações ordenadas, éticas, econômicas e adequada salvaguarda contra perdas, mau uso ou dano.
- **Comunicação-** confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento das obrigações de *accountability*
- **Conformidade** aderência às leis e regulamentações aplicáveis à entidade, e às normas, políticas, aos planos e procedimentos da própria organização.

Apetite a risco aspectos qualitativos (elevado, moderado e baixo), aspectos quantitativos (equilibra as metas de crescimento e retorno aos riscos).

Tolerância a riscos mensurais de preferência, nas mesmas unidades que os objetivos correlatos e alinham-se ao apetite a riscos.

COSO II – 2º Componente: Fixação dos Objetivos

Tolerância a Riscos

Alta tolerância a riscos

Baixa tolerância a riscos

Objetivo

Tolerância a riscos representa o nível aceitável de variação em relação à meta para o cumprimento de um objetivo específico.

Objetivo Estratégico – Seges:

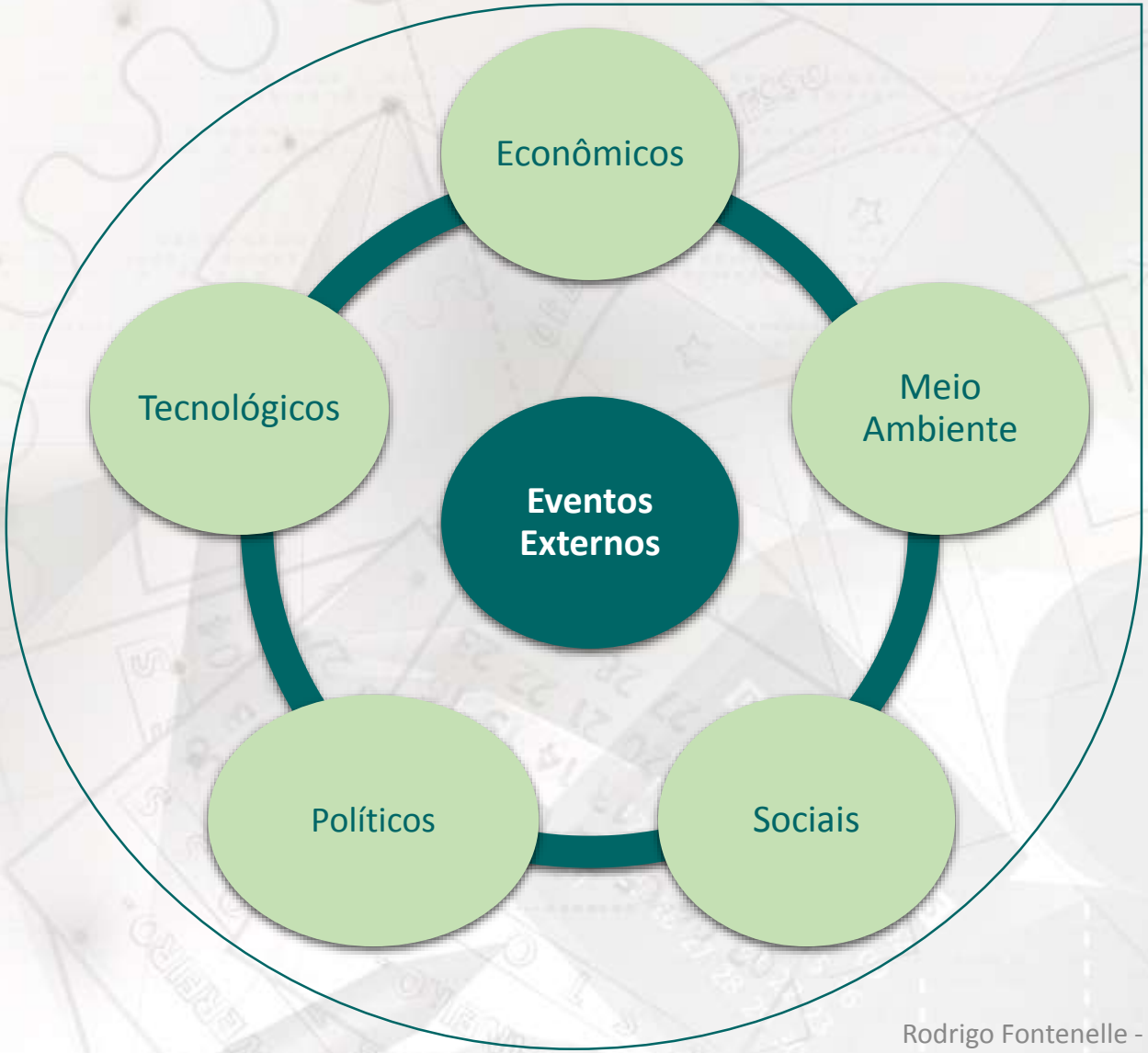
Aprimorar a gestão e elevar a efetividade e a transparência das transferências voluntárias

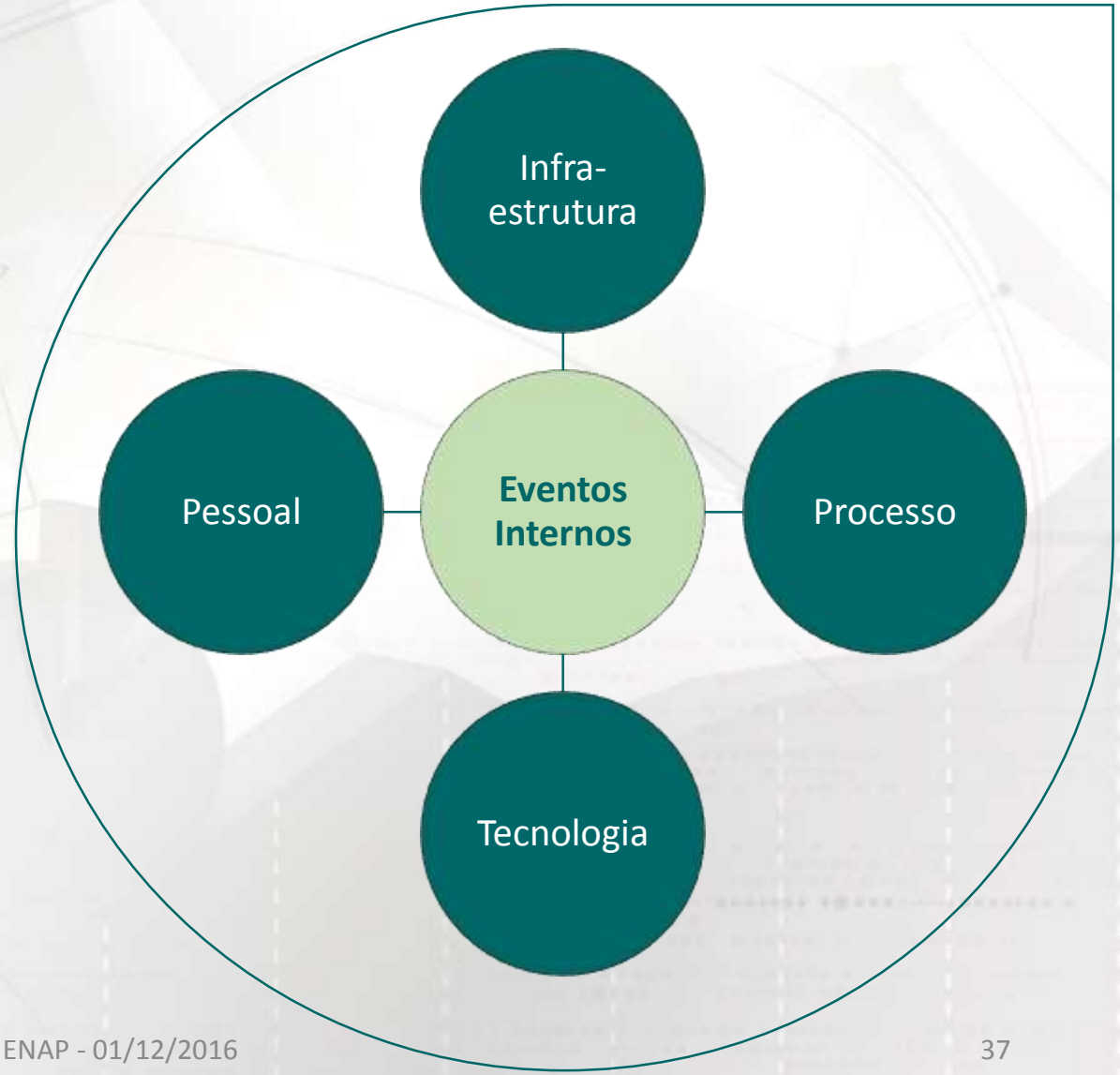
COSO – 3º Componente: Identificação de Eventos

Os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. As **oportunidades são canalizadas para os processos de estabelecimento de estratégias** da administração ou de seus objetivos. Enquanto os **riscos afetam negativamente a realização dos objetivos**.

Eventos: situações em potencial, que ainda não ocorreram, mas que **podem causar impacto na consecução dos objetivos** da organização, caso venham a ocorrer.

COSO – 3º Componente: Identificação de Eventos





COSO II – 3º Componente: Identificação de Eventos

Eventos Externos - Seges:

Econômico: contingenciamento

Político: não aprovação de alteração de estrutura legal

Eventos Internos - Seges:

Pessoal: alto *turnover*

Infra-estrutura: obsolescência de equipamentos

Tecnologia: atraso na finalização do novo sistema

COSO – 3º Componente: Identificação de Eventos

Análise de SWOT

S *– Strengths (Forças)*

W *– Weaknesses (Fraquezas)*

O *– Opportunities (Oportunidades)*

T *– Threats (Ameaças)*

I. Ambiente externo: oportunidades e ameaças (SWOT)

II. Ambiente interno: pontos fortes e fracos (**SW**OT)

Análise SWOT é uma **ferramenta utilizada para fazer análise de cenário** (ou análise de ambiente). As informações obtidas sobre o ambiente interno e externo, contribuem na identificação dos riscos e na escolha das respostas aos riscos.

COSO – 4º Componente: Avaliação de Riscos

Análise dos riscos relevantes para **o alcance dos objetivos e metas da entidade**, com vistas a dar a resposta apropriada**.**

Risco: evento futuro e incerto que, caso ocorra, pode **impactar negativamente** o alcance dos objetivos da organização.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

(IN Conjunta MP/CGU Nº 01/2016)

Os riscos são analisados, considerando a **probabilidade** e o **impacto** como base para determinar o modo pelo qual deverão ser geridos. Também são avaliados quanto à sua condição de **inerentes e residuais**

COSO II – 4º Componente: Avaliação de Riscos

Princípios[1]

- Define objetivos relevantes
- Identifica e analisa riscos
- Avalia o risco de fraude
- Identifica e analisa alterações que podem impactar significativamente o sistema de controle interno

[1] COSO 2013

COSO – 4º Componente: Avaliação de Riscos

Identificar riscos de negócio relevantes para os objetivos da organização

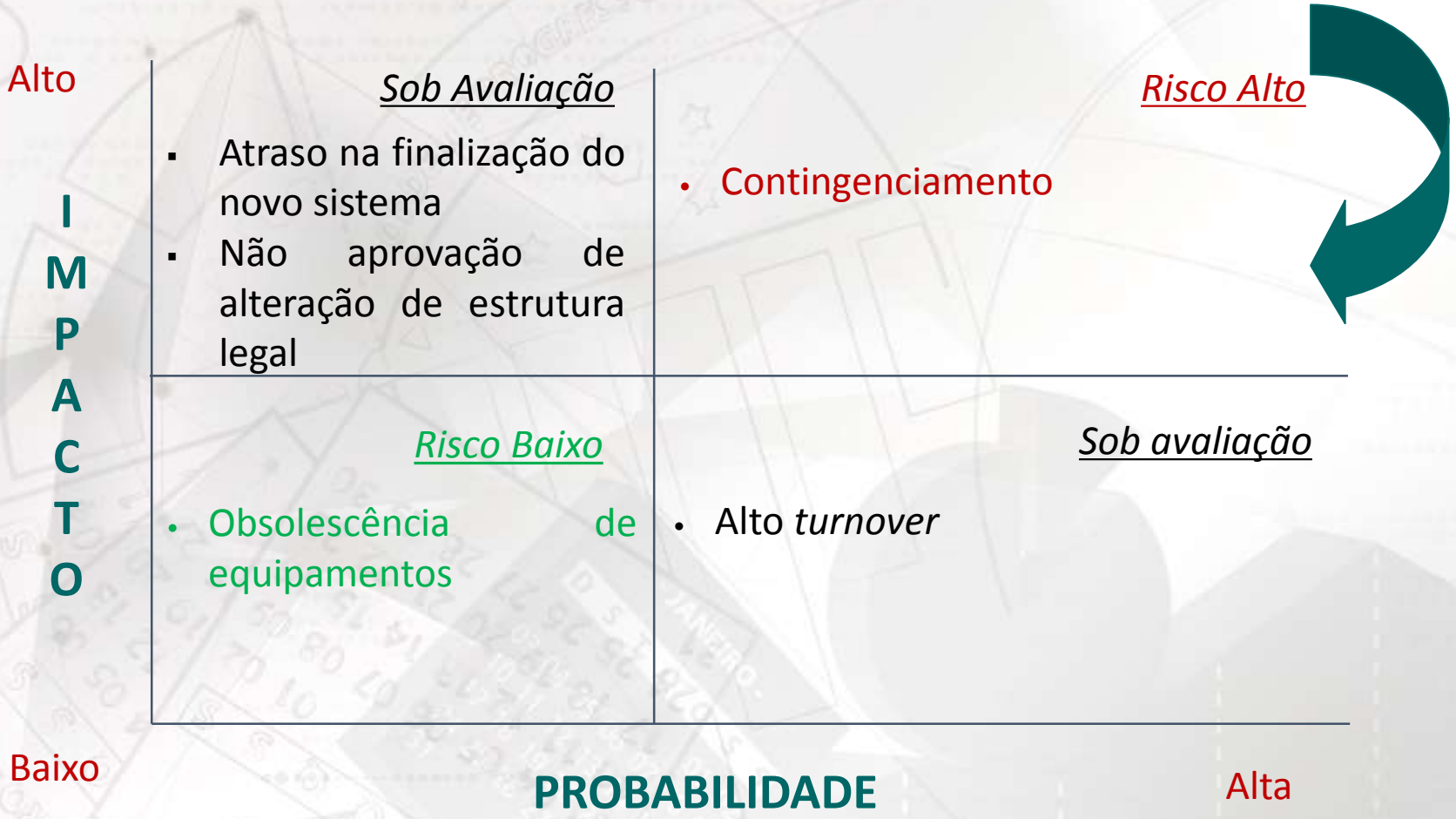
Estimar a significância dos riscos

Avaliar a probabilidade de sua ocorrência

Decidir sobre ações em resposta a esses riscos

COSO – 4º Componente: Avaliação de Riscos

Exemplo: Aprimorar a gestão e elevar a efetividade e a transparência das transferências voluntárias



COSO – 4º Componente: Avaliação de Riscos

Os riscos são avaliados com base em suas características inerentes e residuais

Risco Inerente

é o **risco que uma organização terá de enfrentar na falta de medidas** que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos.

Risco Residual

é aquele que **ainda permanece após a resposta da administração**. A avaliação de riscos é aplicada primeiramente aos riscos inerentes.

COSO – 4º Componente: Avaliação de Riscos

Exemplo de avaliação de Riscos:

- ✓ Um ganho certo de R$ 250,00 ou 25% de chance de ganhar R$ 1.000,00, e 75% de chance de não ganhar nada.
- ✓ Um prejuízo certo de R$ 750,00, ou 75% de chance de perder R$ 1.000,00 e 25% de chance de não perder nada.
- ✓ Segundo a Teoria das Expectativas, as pessoas não desejam colocar em risco o que já tem ou pensam que podem ter, mas apresentam maior tolerância a riscos quando podem minimizar prejuízos.

COSO – 5º Componente: Resposta a Risco

Após a avaliação dos riscos, a Administração determina como responderá aos riscos.

As respostas incluem **evitar, reduzir, compartilhar** ou **aceitar** os riscos.

Identifica as oportunidades e chega a uma visão de toda organização – **visão de portfólio, determinando** se os riscos **residuais** gerais são **compatíveis** com a **tolerância a riscos** e com o **apetite a riscos** da organização.

Respostas aos riscos: **evitar, reduzir ou compartilhar/transferir ou aceitar**, desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco.

COSO – 5º Componente: Resposta a Risco

Evitar
- Suspensão das atividades.

Reduzir
- Adoção de procedimentos de controle para minimizar a probabilidade e/ou o impacto do risco.

Compartilhar
- Redução da probabilidade ou do impacto por meio de transferência.

Aceitar
- Não adotar medidas mitigadoras.

COSO – 5º Componente: Resposta a Risco

Impacto	Probabilidade
Alto Impacto / Baixa Probabilidade ▸ Compartilhar	**Alto Impacto / Alta Probabilidade** ▸ Evitar ▸ Compartilhar ▸ Reduzir
Baixo Impacto / Baixa Probabilidade ▸ Aceitar	**Baixo Impacto / Alta Probabilidade** ▸ Reduzir

COSO – 6º Componente: Atividades de Controle

São as políticas e procedimentos que contribuem para assegurar se:

- ✓ os **objetivos** estão sendo **alcançados**
- ✓ as **diretrizes** administrativas estão sendo **cumpridas**
- ✓ estão sendo realizadas as ações necessárias para **gerenciar os riscos** com vistas à consecução dos objetivos da entidade

Se estabelecidas de forma tempestiva e adequada, podem vir a **prevenir ou administrar os riscos** inerentes ou em potencial da entidade. Não são exclusividade de determinada área da organização, sendo realizadas em todos os níveis.

As **políticas** e **procedimento**s são estabelecidos e implementados para **assegurar que as respostas aos riscos** sejam executadas com eficácia.

COSO II – 6º Componente: Atividades de Controle

Princípios[1]

Seleciona e implementa atividades de controle

Seleciona e implementa atividades de controle sobre a tecnologia

Baseia-se em políticas e procedimentos

[1] COSO 2013

COSO – 6º Componente: Atividades de Controle

São exemplos de **tipologias de atividades de controle**:

✓ Atribuição de autoridade e limites de alçada	✓ Revisões da Alta Administração
✓ Revisão de superiores	✓ Normatização Interna
✓ Autorizações e Aprovações	✓ Controles Físicos
✓ Segregação de Funções	✓ Capacitação e Treinamento
✓ Verificações	✓ Conciliações
✓ Indicadores de Desempenho	✓ Revisão de Desempenho Operacional
✓ Programas de Contingência	✓ Planos de Continuidade dos Negócios

COSO – 7º Componente: Informação e Comunicação

Identificação e comunicação **oportuna** das informações permite:

- ✓ cumprimento das responsabilidades;
- ✓ tomada de decisões tempestivas;
- ✓ o melhor aproveitamento de recursos;
- ✓ ganhos operacionais.

As **informações** devem ser coletadas e comunicadas de forma coerente e tempestiva. **TODOS** os níveis de uma organização devem receber informações, para identificar, avaliar e responder a riscos.

A **comunicação eficaz** também ocorre em um sentido mais amplo, fluindo **em todos níveis da organização.**

COSO II – 7º Componente: Informação e Comunicação

Princípios[1]

- Usa informação relevante
- Comunica internamente
- Comunica externamente

[1] COSO 2013

COSO – 7º Componente: Informação e Comunicação

- As informações são necessárias em todos os níveis de uma organização, para identificar, avaliar e responder a riscos
  Requisitos: **pontualidade e profundidade**
- Comunicação interna: papéis e responsabilidades
- Comunicação externa: *stakeholders* (clientes, fornecedores, sociedade)
- Infra-estrutura de TI: suporte à conversão de dados em informações

COSO – 8º Componente: Monitoramento

A integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias.

O monitoramento é realizado através de:

- ✓ Atividades gerenciais contínuas
- ✓Avaliações independentes.
- ✓Auto avaliações.

Atividades gerenciais contínuas ou **avaliações independentes** ou de **ambas as formas.**

COSO II – 8º Componente: Monitoramento

Princípios[1]

Concebe e realiza avaliações contínuas e/ou autónomas

Avalia e comunica eventuais deficiências

[1] COSO 2013

COSO – 8º Componente: Monitoramento

Objetiva verificar se os Controles Internos são adequados e eficientes, examinando:

- os 8 componentes estão presentes e funcionando como planejado
- o alcance dos objetivos operacionais
- as informações dos relatórios e sistemas corporativos confiáveis
- o cumprimento de leis, normas e regulamentos

Compreende o acompanhamento da qualidade do controle interno, visando assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos.

Atributos desejáveis para Gerenciar Riscos

Capacidade de abordar os problemas a partir de perspectiva de sistemas, em vez de abordagem unidimensional

Capacidade de assumir seus erros e de aprender com eles

Capacidade de trabalhar com equipes interdisciplinares e multifuncionais

Competências gerenciais profissionais que lhe permitam desenvolver sistemas, estruturas e incentivos organizacionais para a implementação de programas de gestão de riscos

Desafios

Conscientizar os gestores das áreas de que eles são os responsáveis por gerenciar os riscos, com apoio da equipe de gestão de risco

Inserir no trabalho diário dos gestores o gerenciamento de risco

Comunicar continuamente a necessidade e o papel de cada gestor em processos de gestão de riscos

Modelo de Gestão de Integridade, Riscos e Controles Internos da Gestão

Assessoria Especial de Controle Interno

AECI/GM/MP

Agenda

- Visão Geral do Modelo
- Proposição de Política
- Metodologia
- Estrutura
- Solução Tecnológica
- Cronograma de Desenvolvimento

“Existe o risco que você não pode jamais correr, e existe o risco que você não pode deixar de correr.” (Peter Drucker)

OBRIGADO!

Ministério do Planejamento, Desenvolvimento e Gestão – MP
Gabinete do Ministro – GM
Assessor Especial de Controle Interno – AECI

Rodrigo Fontenelle de Araújo Miranda, CGAP, CRMA, CCSA
rodrigo.miranda@planejamento.gov.br
Fone: 2020.4020