Enap Escola Nacional de Administração Pública

Implementando a Gestão de riscos no setor público

Módulo 2 Estrutura do COSO ERM

Brasília - 2018

Conteúdo para impressão

Fundação Escola Nacional de Administração Pública

Presidente
Francisco Gaetani

Diretor de Educação Continuada
Paulo Marques

Coordenadora-Geral de Educação a Distância
Natália Teles da Mota Teixeira

Conteudista
Rodrigo Fontenelle de Araújo Miranda

Desenvolvimento do curso realizado no âmbito do acordo de Cooperação Técnica FUB/CDT/Laboratório Latitude e Enap.

Enap Escola Nacional de Administração Pública
Diretoria de Educação Continuada
SAIS - Área 2-A - 70610-900 — Brasília, DF
Telefone: (61) 2020 3096 - Fax: (61) 2020 3178

SUMÁRIO

Enap
Enap
Enap

Módulo 2 Estrutura do COSO ERM

1. Introdução

Olá! Seja bem-vinda (o) ao Módulo 2!

Nesse módulo, entre outros assuntos, conheceremos a estrutura do COSO ERM. Vamos continuar nossos estudos? Então mãos à obra!

Você aprendeu que COSO (*Committee of Sponsoring Organizations*) é o Comitê das Organizações Patrocinadoras, da Comissão Nacional sobre Fraudes em Relatórios Financeiros. E que esse comitê definiu gerenciamento de riscos corporativos como um processo que deve ser conduzido por todos os agentes da administração. Não deixe de reler o módulo 1 para retomar integralmente esse conceito fundamental para nossos estudos!

De acordo com o COSO ERM, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização.

Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e é classificada em quatro categorias:

- 1 - Estratégicos – metas gerais, alinhadas com sua missão.
- 2 - Operações – utilização eficaz e eficiente dos recursos.
- 3 - Comunicação – confiabilidade de relatórios.
- 4 - Conformidade – cumprimento de leis e regulamentos aplicáveis.

2. A estrutura do COSO ERM

O COSO ERM definiu oito componentes em sua estrutura, quais sejam:

- Ambiente de controle;
- Fixação de objetivos;
- Identificação de eventos;
- Avaliação de riscos;
- Resposta ao risco;
- Atividades de controle;

- Informações e comunicações;
- Monitoramento.

A figura abaixo representa o Cubo COSO ERM, indicando a relação entre a dimensão dos objetivos da instituição, a dimensão dos níveis da organização e os oito componentes dessa estrutura, vejamos:

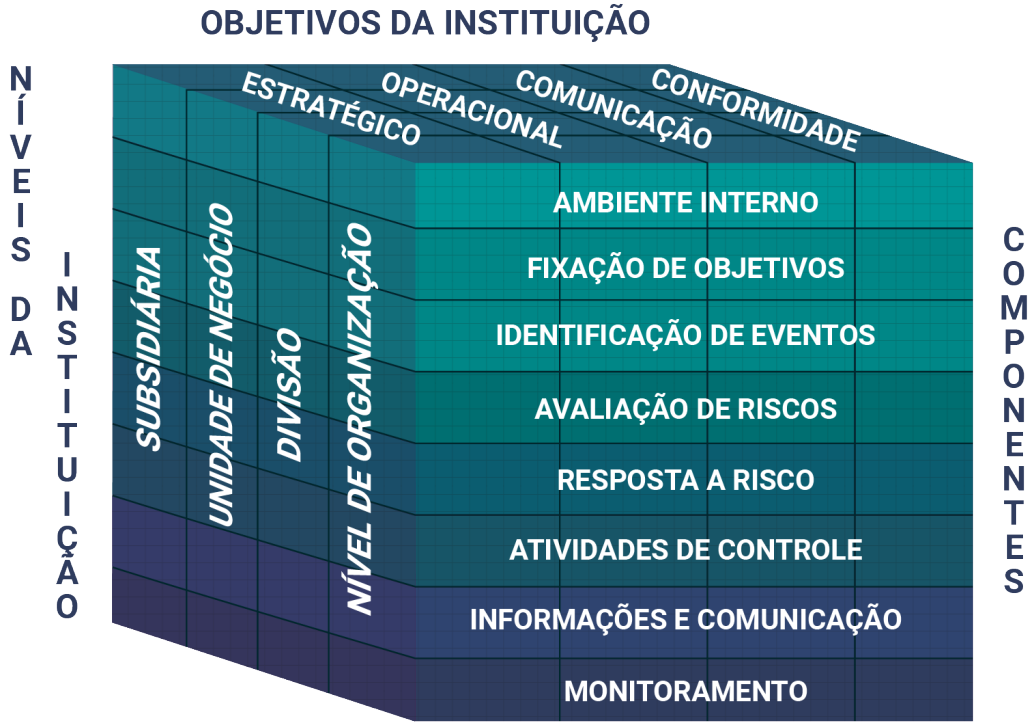

Figura 1: Cubo do Coso

2.1 Ambiente de controle

Este componente está relacionado ao núcleo de qualquer Organização, o pessoal (Recursos Humanos) – atributos individuais, principalmente integridade, valores éticos e competência, e o ambiente no qual operam. Ele provê uma atmosfera na qual as pessoas conduzem suas atividades e cumprem suas responsabilidades de controle, servindo de base para os demais componentes, retrata a "consciência e a cultura de controle" e é afetado fortemente pelo histórico e pela cultura da organização.

Segundo o Instituto de Auditores Internos (IIA), o Ambiente de Controle representa:

Atitudes e ações do Conselho e da Administração em relação à importância dos controles dentro da organização, definindo o tom da organização.

O Ambiente de Controle está intrinsecamente relacionado aos controles não operacionais, que estão fortemente relacionados com os valores das pessoas da organização e são igualmente importantes para gerar um ambiente de controle saudável. Entretanto, não são detectados pelas abordagens e ferramentas tradicionais de auditoria, requerendo técnicas não tão

comumente utilizadas, para que se obtenham evidências suficientes sobre a existência deste componente, tais como a observação do ambiente.

O ambiente de controle deve demonstrar o grau e comprometimento em todos os níveis da administração, com a qualidade do controle interno em seu conjunto. É o principal componente. Os fatores relacionados ao ambiente de controle incluem, dentre outros:

- integridade e valores éticos;
- competência das pessoas da entidade;
- estilo operacional da organização;
- aspectos relacionados com a gestão;
- forma de atribuição da autoridade e responsabilidade.

2.2 Fixação de objetivos

Definidos pela alta administração, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam influenciar na consecução dos objetivos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

2.3 Identificação de eventos

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

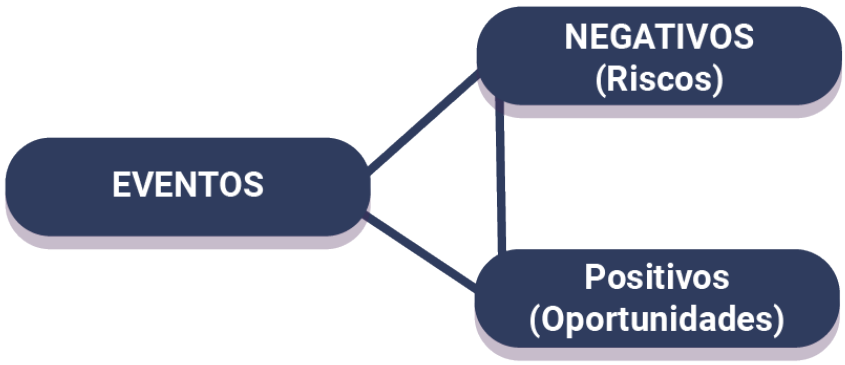

Figura 2: Identificação de Eventos

Por meio da identificação de eventos, é possível planejar o tratamento adequado para as oportunidades e para os riscos, que devem ser entendidos como parte de um contexto, e não de forma isolada.

Isso porque, muitas vezes, um risco que parece trazer grande impacto pode ser minimizado pela existência conjunta de uma oportunidade.

Após a identificação de eventos, separando-se as oportunidades dos riscos, vamos atuar sobre esses últimos, por meio da avaliação de riscos, quando determinaremos a forma de tratamento para cada risco identificado, e qual o tipo de resposta a ser dada a esse risco.

2.4 Avaliação de risco

A organização deve estar consciente dos riscos relevantes que envolvem o negócio, bem como deve gerenciar esses riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Assim, é pré-requisito o estabelecimento, por parte da organização, de objetivos estratégicos alinhados a sua Missão e Visão, para que ela opere de forma conjunta e organizada.

A gestão de riscos (identificação e avaliação de riscos e definição de respostas, dentre elas, controles) interage com o Planejamento Estratégico, à medida que a organização, ao identificar e tratar os riscos e implementar controles internos focados nesses riscos, estará aumentando a probabilidade de alcance dos objetivos definidos. Ou seja, a gestão de riscos é considerada uma boa prática de Governança da organização, ao incluir aspectos relacionados à *accountability* (prestação de contas, no sentido de que a gestão está alinhada às diretrizes estratégicas), à transparência (que é um pré-requisito para uma adequada prestação de contas), dentre outros.

2.5 Resposta aos riscos

Para cada risco identificado, será prevista uma resposta que poderá ser: evitar, aceitar, compartilhar ou reduzir. Vejamos, de acordo com o COSO, o que sugere cada uma dessas respostas:

- evitar: sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável;
- reduzir: diminui o risco residual a um nível compatível com as tolerâncias desejadas ao risco;
- compartilhar: uma ação é tomada para transferir ou compartilhar riscos em toda a entidade ou com partes externas;
- aceitar: indica que o risco inerente já esteja dentro das tolerâncias ao risco.

É importante observarmos que aceitar o risco é uma forma de responder ao risco. Ou seja, se você “não fizer nada” em relação ao risco, você ainda estará respondendo a ele, desde que essa inércia seja consciente. Isso pode vir a ocorrer, por exemplo, quando o custo de implementação de uma medida qualquer para responder a determinado risco fique muito alto, maior até do que os benefícios que a resposta traria para a organização.

A imagem abaixo demonstra as quatro possibilidades de resposta aos riscos:

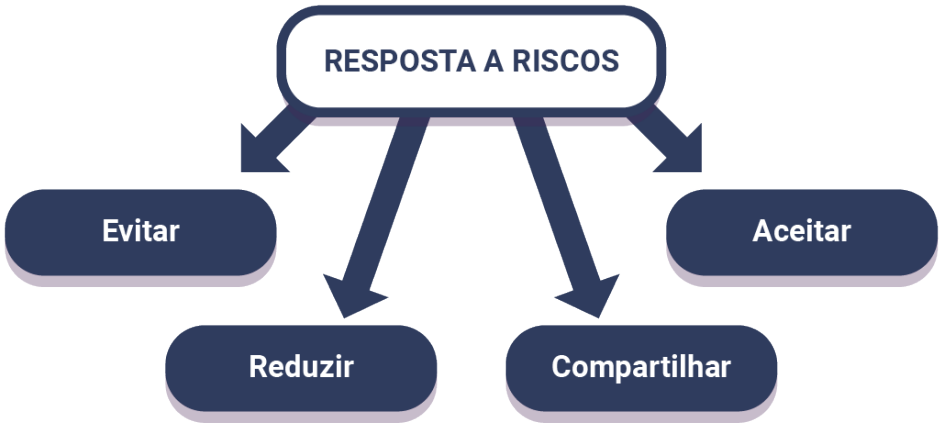

Figura 3: Resposta a riscos

IMPORTANTE

Em relação a riscos, é importante apresentar dois conceitos, vejamos:

- **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.

2.6 Atividades de controle

As Atividades de Controle geralmente estão expressas em políticas e procedimentos de controle, que devem ser estabelecidos e aplicados para auxiliar e assegurar que ações identificadas pela administração, como necessárias para tratar os riscos relacionados ao cumprimento dos objetivos da organização, sejam realizadas de forma eficaz. As atividades de controle estão comumente voltadas para três categorias de riscos: de processo ou operacionais; de registros; e de conformidade. Assim, as atividades de controle contribuem para assegurar que:

- os objetivos sejam alcançados;
- as diretrizes administrativas sejam cumpridas;
- as ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da entidade estejam sendo implementadas.

As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, podem vir a prevenir ou administrar os riscos inerentes ou em potencial da entidade. São exemplos de tipologias de atividades de controle:

- atribuição de autoridade e limites de alçada;
- revisão segregada;

- autorizações e aprovações;
- controles físicos;
- segregação de funções;
- verificações;
- conciliações;
- indicadores de desempenho;
- revisão de desempenho operacional;
- programas de contingência e planos de continuidade dos negócios.

IMPORTANTE

As atividades de controle não são exclusividade de determinada área da organização, sendo realizadas em todos os níveis.

2.7 Informação e comunicação

Abrangem informações e sistemas de comunicação, permitindo que as pessoas da organização coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações.

Toda informação relevante, relacionada aos objetivos, riscos e controles, seja capturada e comunicada por toda a organização.

A organização também deve possuir mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir externamente aqueles que sejam relevantes aos stakeholders, inclusive à sociedade, que, no caso das organizações públicas, pode ser considerada a principal parte interessada.

A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, econômicos, operacionais e estratégicos. Deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados e vice-versa –, pois determinados assuntos são mais bem visualizados pelos integrantes dos níveis mais subordinados, que estão mais diretamente ligados aos processos organizacionais

2.8 Monitoramento

Compreende o acompanhamento da qualidade do controle interno, visando a assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos. Pressupõe uma atividade desenvolvida ao longo do tempo.

O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode “reagir” de

forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento pode ser realizado por meio de:

- atividades contínuas; e
- avaliações independentes (por exemplo, auditorias internas e externas);

As atividades contínuas são incorporadas às demais atividades normais da organização, e as avaliações independentes garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Modernamente também são utilizadas as autoavaliações, processo que pode ter um grande auxílio dos auditores, pois esses podem partir dessa autoavaliação para realizarem suas avaliações independentes, no sentido de confirmarem o que foi autoavaliado.

O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerão basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento.

Diferentemente das atividades de controle, que são concebidas para dar cumprimento aos processos e às políticas da organização e visam a tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias.

IMPORTANTE

Os riscos e as oportunidades mudam ao longo do tempo e devem ser monitoradas para que a organização possa realizar os ajustes necessários.

3. Revisando o módulo

Neste módulo, abordamos a estrutura do COSO ERM, revise os tópicos estudados que merecem destaque:

- No COSO II, as quatro categorias de objetivos 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.

- No COSO II, temos oito componentes inter-relacionados, são eles: Ambiente Interno, Fixação de Objetivos, Identificação de Eventos, Avaliação de Riscos, Resposta aos Riscos, Atividades de Controle, Informação e Comunicação e Monitoramento.

- Os riscos são avaliados considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser geridos. As respostas incluem evitar, reduzir, compartilhar ou aceitar os riscos.

Concluímos a leitura do módulo 2! Assista aos vídeos e realize a Atividade Avaliativa deste módulo, para concluí-lo com êxito. É fundamental que revise o conteúdo antes de prosseguir para o próximo módulo, pois apresentaremos as etapas da Metodologia de Gerenciamento de Riscos do MP.

Enap
Enap
Enap

Referências

ABNT. Associação Brasileira de Normas Técnicas. **Gestão de Riscos**: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000. 1. ed. São Paulo: ABNT, 2009.

AHP. Analytic Hierarchy Process. **Excel MS Excel 2010.** Modelo AHP desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel. Disponível em: <http://bpmsg.com>. Acesso em 3 out. 2017. Versão de livre uso.

BB. Banco do Brasil. Diretoria de Controles Internos. **Priorização de Processos, Escopo de Atuação**. Visita Técnica em 26 jul. 2015.

BCB. Banco Central do Brasil. **Fundamentos de Gestão de Riscos Não-Financeiros**. Disponibilizada pela UniBacen. Curso realizado de 30/06 a 06/07/2015.

_____. Ministério do Planejamento. **Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos**. Programa Gespública. Secretaria de Gestão Pública. Brasília, 2013.

_____. Ministério do Planejamento. **O Modelo de Excelência em Gestão Pública. Programa Gespública.** Secretaria de Gestão Pública. Brasília, 2014a.

_____. Ministério do Planejamento. **Instrumento para Avaliação da Gestão Pública. Programa Gespública.** Secretaria de Gestão Pública. Brasília, 2014b.

_____. Tribunal de Contas da União. Processo TC 020.905/2014-9. **Relatório de Levantamento de Auditoria,** Acórdão nº 927/2015 - TCU Plenário, Brasília, 2014c.

_____. Tribunal de Contas da União. **Avaliação de controles internos na administração pública federal,** 2012. Disponível em <http://portal2.tcu.gov.br/portal/pls/portal/docs/2436815.PDF>. Acesso em 14. set. 2013.

BRITO, Claudenir; FONTENELLE, Rodrigo. **Auditoria privada e governamental:** Teoria de forma objetiva e mais de 500 questões comentadas. 3. ed. Niterói: Impetus, 2016.

COSO ERM. **Gerenciamento de Riscos Corporativos** - Estrutura Integrada, 2004.

COSO. **Gerenciamento de Riscos Corporativos** – Estrutura Integrada. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

IIA. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.** Disponível em: <https://na.theiia.org/standards-guidance/Public%20Documents>. Acesso em: 17. nov. 2015.
IBGC. INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de Orientação para Gerenciamento de Riscos Corporativos.

INTOSAI GOV 9100. **Guidelines for Internal Controls Standards for the Public Sector.** 2004. Disponível em: <http://www.intosai.org/en/issai-executive-summaries/intosai- guidance-for-good-governance-intosai-gov.html >. Acesso em: 28 out. 2015.

ISO. International Organization for Standardization. **Risk Management System – Principles and Guidelines**. ISO 31000. Tradução: Associação Brasileira de Normas Técnicas (ABNT) Projeto 63:000.01- 001. Agosto, 2009.

_____. **Vocabulary for Risk Management,** ISO Guide 73, 2009.

KPMG. **The Audit Committee's Role in Control and Management of Risk.**

MIRANDA, Rodrigo F. A. **Implementando a Gestão de Riscos no Setor Público**. Belo Horizonte: Ed. Fórum, 2017.