PROCEDIMENTOS DE GESTÃO DE RISCOS – COSO ERM
WHITE TRATORES SERVICOS DE TERRAPLENAGEM EIRELI

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

SUMÁRIO

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

1. Introdução

COSO (Committee of Sponsoring Organizations) é o Comitê das Organizações Patrocinadoras, da Comissão Nacional sobre Fraudes em Relatórios Financeiros.
Este comitê definiu o gerenciamento de riscos corporativos como um processo que deve ser conduzido por todos os agentes da administração.

De acordo com o COSO ERM (*enterprise risk management* - gerenciamento de riscos corporativos), 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 é definida em oito componentes:

• 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:

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

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.

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;

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

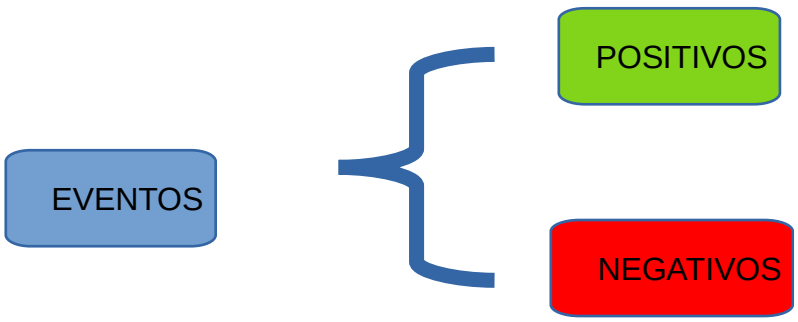
• forma de atribuição da autoridade e responsabilidade.

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.



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

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

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.

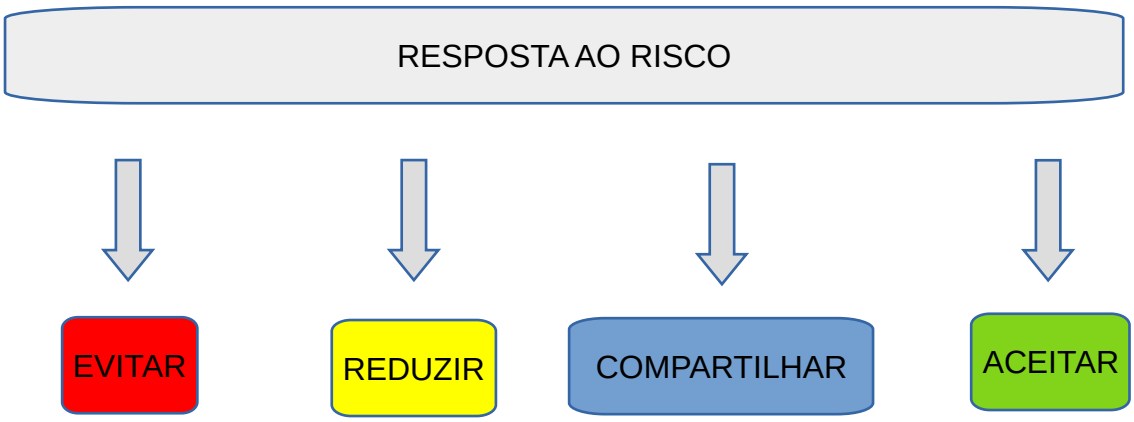
2.5 Resposta aos riscos

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:

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade



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;

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

• revisão de desempenho operacional;
• programas de contingência e planos de continuidade dos negócios.

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;
• 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

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

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.

3.Glossário

Apetite a Riscos – A quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão).

Conformidade – empregado com os “objetivos” e relacionado com o cumprimento de leis e regulamentos aplicáveis.

Controle Interno – Processo efetuado pelo conselho, administração ou qualquer outro funcionário de uma empresa, desenhado para fornecer garantia razoável em relação à realização dos objetivos nas seguintes categorias:

- Eficácia e eficiência das operações.
- Confiabilidade dos relatórios financeiros.
- Conformidade com leis e regulamentos aplicáveis.

Desenho – 1. Propósito. Conforme utilizado na definição, gerenciamento de riscos corporativos tem a finalidade de identificar os eventos em potencial capazes de afetar a empresa e gerenciar o risco de modo a mantê-lo em conformidade com o apetite a riscos da referida organização, possibilitar garantia razoável em relação à realização dos objetivos. 2. Plano; o modo pelo qual um processo deve operar, em comparação ao modo pelo qual efetivamente opera.

Evento – Incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

Impacto – Resultado ou efeito de um evento. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos correlatos de uma empresa.

Data	Versão	Descrição	Autor	Revisor
11/05/2021	v1.0	Criação	CONSULTRON	Consultoria de Capacitação Ltda
30/06/2021	v1.1	Validação	CONSULTRON	Departamento de Integridade WHITE TRATORES
10/05/2023	V2.0	Alteração	WHITE TRATORES	Participantes do Departamento de Integridade

Integridade – A qualidade ou o estado de possuir princípios morais íntegros; retidão, honestidade e sinceridade; o desejo de fazer aquilo que é certo, professar e viver de acordo com uma série de valores e expectativas.

Oportunidade – A possibilidade que um evento ocorrerá e afetará favoravelmente a realização dos objetivos.

Política – A administração estabelece aquilo que deverá ser feito para efetuar o controle. Uma política serve de base para a definição dos procedimentos e sua implementação.

Probabilidade - A possibilidade de ocorrência de um dado evento. Os termos podem adquirir conotações mais específicas como indicar “possibilidade” de que um dado evento ocorrerá em termos qualitativos, como elevada, média e reduzida, ou outras escalas de julgamento; e “probabilidade” indicando uma medida quantitativa, como porcentagem, frequência de ocorrência ou outra unidade numérica de medida.

Risco – A possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos.

Risco Inerente – O risco que se apresenta a uma organização na ausência de qualquer medida gerencial que poderia alterar a probabilidade ou o impacto de um risco.

Risco Residual – O risco que resta após a administração ter adotado medidas para alterar a probabilidade ou o impacto dos riscos.

Tolerância a Riscos – A variação aceitável relativa à realização de um objetivo.

WHITE TRATORES SERVICOS DE TERRAPLENAGEM EIRELI:04000710000172

Assinado de forma digital por WHITE TRATORES SERVICOS DE TERRAPLENAGEM EIRELI:04000710000172
Dados: 2023.05.15 10:28:41 -03'00'

WHITE TRATORES SERVIÇOS DE TERRAPLANAGEM EIREL

CNPJ: 04.000.710/0001-72