

GOVERNANÇA EM TECNOLOGIA DA INFORMAÇÃO – RISCOS E CONTROLES

A series of horizontal lines in teal and light blue colors, with varying lengths and thicknesses, extending from the left edge of the slide towards the right, positioned below the main title.

Princípios da governança



Governar é a habilidade de comandar por meio do poder, no entanto, isso não assegura o alcance do sucesso. Todo líder inicia estabelecendo sua visão e angariando seguidores. Governar é, ademais, estabelecer e manter uma estrutura organizacional que seja eficiente e eficaz.



Governança consiste na configuração das interações entre indivíduos, procedimentos e tecnologia dentro do contexto de uma empresa.



Para compreender de maneira mais aprofundada os elementos ligados à gestão corporativa, é crucial entender certos princípios fundamentais para a criação, crescimento e continuidade de uma organização.

Conceitos relevantes

- **Missão:** é a descrição por escrito das intenções e ambições de uma organização, com o propósito de disseminar o ethos da empresa (identidade, cultura e valores fundamentais adotados e promovidos), o qual está intrinsecamente ligado à sua visão e à de todos os membros da instituição.
- **Transparência:** de acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), implica que o principal executivo (CEO) deve disponibilizar prontamente todas as informações relevantes, para além das obrigatórias por lei ou regulamentação, a todas as partes interessadas, priorizando a substância sobre a forma. A diretoria deve buscar a clareza e a concisão nas informações, utilizando uma linguagem acessível ao público-alvo.

- **Equidade:** conforme definido pelo IBGC, se caracteriza pelo tratamento imparcial e igualitário de todos os grupos minoritários, independentemente de serem acionistas ou outras partes interessadas, como funcionários, clientes, fornecedores ou credores. Comportamentos ou políticas discriminatórias, independentemente da justificativa, são completamente inadmissíveis.
- **Prestação de contas:** segundo o IBGC, implica que os agentes envolvidos na governança corporativa devem prestar contas de suas ações àqueles que os elegeram e são plenamente responsáveis por todas as decisões tomadas durante o exercício de seus cargos.

- **Responsabilidade corporativa:** de acordo com IBGC, implica que conselheiros e executivos têm a responsabilidade de assegurar a continuidade das organizações, promovendo uma visão de longo prazo e sustentabilidade.
 - Portanto, é fundamental que considerem aspectos sociais e ambientais na formulação de estratégias de negócios e operações.
 - A responsabilidade corporativa transcende a estratégia empresarial, abrangendo todos os vínculos da empresa com a comunidade na qual está inserida.

Vídeo

- **O QUE É GOVERNANÇA CORPORATIVA - Perguntas e Respostas para Você!**
 - <https://www.youtube.com/watch?v=-0t73oMFW6Y>

O que é governança de TI?

- É o processo de tomada de decisões relacionadas aos investimentos em Tecnologia da Informação (TI), abrange aspectos como a metodologia de tomada de decisões, os responsáveis pela tomada de decisões, a atribuição de responsabilidades e a forma como os resultados são avaliados e acompanhados.
- A Governança de TI é um componente integrante da governança corporativa. Dado que os dados financeiros das empresas são armazenados em sistemas de informação, os gestores de negócios necessitam de garantias quanto à confiabilidade dessas informações para embasar decisões apropriadas.

- A função da Governança de TI é estabelecer controles que assegurem que a TI opere da maneira mais transparente possível perante os stakeholders, como executivos, conselho de administração e acionistas. Isso visa promover a confiança e a integridade no uso da tecnologia da informação na organização.





Imagem adaptada de: FEELY, Dan. Getting Governance Right. Info Source, v. VII, n. 3, dez 2007. Disponível em: http://www.transforming.com/tsi_news/best_consulting_firm_newsletters_december07.html.

Governança Corporativa

Ativos
Humanos

Ativos
Financeiros

Ativos Físicos

Propriedade
Intelectual

Relaciona-
mento



Governança de TIC

Alinhamento
com o Negócio



Controles
Robustos

Eficiência
Organizacional

Decisões que devem ser tomadas

Princípios de TI: afirmações em um nível elevado que delineiam como a Tecnologia da Informação é empregada para apoiar as operações da organização.

Arquitetura de TI: engloba políticas, diretrizes e opções técnicas destinadas a padronizar e integrar dados, aplicações e procedimentos de negócios.

Estratégias de infraestrutura: abrangem as definições relativas aos serviços de TI a serem oferecidos, bem como as estratégias para a aquisição, prestação e administração desses serviços.

Priorização de Investimentos: envolve o estabelecimento de critérios para a seleção e gerenciamento do portfólio de projetos de TI na organização.

Componentes da governança de TI

- **Estrutura**

- Quem toma as decisões?
- Quais estruturas organizacionais estão envolvidas, quem participa e quais são suas responsabilidades?

- **Processos**

- Como as decisões de investimento são tomadas?
- Quais são os processos para proposta, aprovação e priorização dos investimentos em TI?

- **Comunicação**

- Como as decisões são comunicadas?
- Como os resultados dos investimentos em TI são monitorados, medidos e comunicados?

Estruturas de governança de TI

- **O Papel do CIO:** O CIO tem uma ligação direta com o mais alto líder da organização, participando ativamente de discussões estratégicas.
- **Comitês:** compostos por representantes da alta administração, do departamento de TI e das unidades de negócios, para tomar decisões sobre assuntos específicos.
- **Papeis Específicos/Funções designadas:**
 - **Gestor da governança de TI:** com o foco contínuo nessa área.
 - **Gerentes de relacionamento:** encarregados de traduzir as implicações da governança de TI para as unidades de negócios e, reciprocamente, de traduzir as necessidades dessas unidades para a área de TI.

Processos de governança de TI

- **Gestão de portfólio:** Isso envolve a administração unificada dos ativos de Tecnologia da Informação, do conjunto de soluções já em uso e dos projetos em andamento. As decisões são tomadas com base em uma visão abrangente da TI em toda a organização.
- **Gestão de demandas:** Consolida todas as requisições dirigidas ao setor de Tecnologia da Informação, abrangendo desde as operações cotidianas até as solicitações de caráter estratégico. Isso simplifica o desenvolvimento de uma visão abrangente da área de TI.

- **Acordos de nível de serviço (SLA - Service Level Agreement):** Estabelecem de maneira clara as condições para a prestação de serviços de TI, abrangendo também os custos envolvidos, a fim de possibilitar a tomada de decisões informadas a respeito desses serviços.

Exemplo de como elaborar um SLA

#	Pergunta	Resposta	Prioridade
A	O problema/solicitação/dúvida impede que a empresa realize seus processos básicos (faturamento / pagamento)?	Sim	Crítica
B	O problema/solicitação/dúvida impede a execução de algum serviço da empresa?	Sim	Crítica
C	O problema/solicitação/dúvida impede que o usuário realize sua função?	Sim	Crítica
D	O problema/solicitação/dúvida do usuário não o impede de realizar as atividades, mas causa retardo na execução das tarefas?	Sim	Alta
E	O problema/solicitação/dúvida do usuário não o impede de realizar as suas atividades, nem causa retardo, mas o ajudaria a fazer o trabalho melhor?	Sim	Média
F	O problema/solicitação/dúvida impede que o usuário realize funções secundárias?	Sim	Média
G	O problema/solicitação/dúvida não se encaixou em nenhuma das categorias? (!) Aqui é preciso ter cuidado com os falsos positivos. Como nossa estrutura de atribuição de prioridade é simples, pode ser que algum item que caia aqui não seja de prioridade baixa. Fique atento!	Sim	Baixa

Exemplo de como elaborar um SLA

Prioridade	Tipo	SLA
Crítica	Incidente que causa parada	30 minutos
Alta	Incidente que não causa parada	120 minutos
Média	Solicitações de instalação e configuração	480 minutos
Baixa	Dúvidas de usuários	840 minutos

Comunicação e governança de TI

- **Balanced Scorecard para TI:** Elaboração de um Balanced Scorecard (BSC) para a área de Tecnologia da Informação (TI) como uma ferramenta para colocar em prática, comunicar e avaliar a estratégia de TI, juntamente com seus mecanismos de governança.
 - **As perspectivas incluídas no BSC são:** criar valor para o negócio, atender às necessidades dos clientes, alcançar excelência operacional e direcionar o futuro.
- **Portal de governança:** Uma plataforma para disponibilizar políticas, padrões, modelos de documentos e relatórios relacionados à gestão de Tecnologia da Informação.

O que é um Balanced Scorecard (BSC)



Um Balanced Scorecard é uma ferramenta de gestão que ajuda as organizações a medir e acompanhar o desempenho de suas atividades de maneira equilibrada e abrangente.



Ele vai além das métricas financeiras tradicionais, como lucro e receita, e inclui indicadores relacionados a aspectos como satisfação do cliente, eficiência interna, aprendizado e crescimento da equipe, além dos financeiros.



O objetivo é fornecer uma visão equilibrada do desempenho da empresa e orientar a tomada de decisões estratégicas com base em múltiplos aspectos. É como um painel de controle que ajuda a empresa a alcançar seus objetivos de forma mais eficaz.

Exemplo de BSC aplicado a área de TI



Exemplo de Portal de Governança



Vídeos

- **GOVERNANÇA DE TI: 5 principais pilares!**
 - <https://www.youtube.com/watch?v=P4nNJk76xFo>
- **Governança Corporativa / Governança de TI**
 - <https://www.youtube.com/watch?v=7MMkTgt9Gvc>

Guias de Boas Práticas de Controle - CobiT e COSO

- **CobiT**, significa "Control Objectives for Information and Related Technologies" (Objetivos de Controle para Tecnologia da Informação e Tecnologias Relacionadas), é um conjunto de boas práticas e diretrizes de controle desenvolvido inicialmente pela ISACA (Information Systems Audit and Control Association) para ajudar as organizações a gerenciar e controlar seus sistemas de tecnologia da informação (TI).

- **COSO**, significa "Committee of Sponsoring Organizations of the Treadway Commission," é uma organização sem fins lucrativos dedicada à melhoria das práticas de governança, gerenciamento de riscos e controle interno nas organizações. O COSO também é conhecido por desenvolver um framework amplamente utilizado chamado "COSO Internal Control - Integrated Framework."

CobiT

- O CobiT fornece um framework abrangente que auxilia na governança e gestão de TI, focando em aspectos como a entrega de valor de TI, gerenciamento de riscos, alinhamento estratégico, otimização de recursos e medição de desempenho.
- Ele se baseia em princípios de controle e fornece um conjunto de processos, práticas e objetivos de controle que ajudam as organizações a garantir que seus sistemas de TI estejam alinhados com as metas e objetivos de negócios.

- O CobiT é amplamente utilizado em todo o mundo como um guia para a gestão de TI, auditoria de sistemas de informação e conformidade regulatória.
- Ele é continuamente atualizado para refletir as mudanças no cenário de TI e nas melhores práticas de governança e gestão. O framework CobiT é uma ferramenta valiosa para garantir a eficácia, eficiência e segurança das operações de TI em uma organização.

Princípios do CobiT

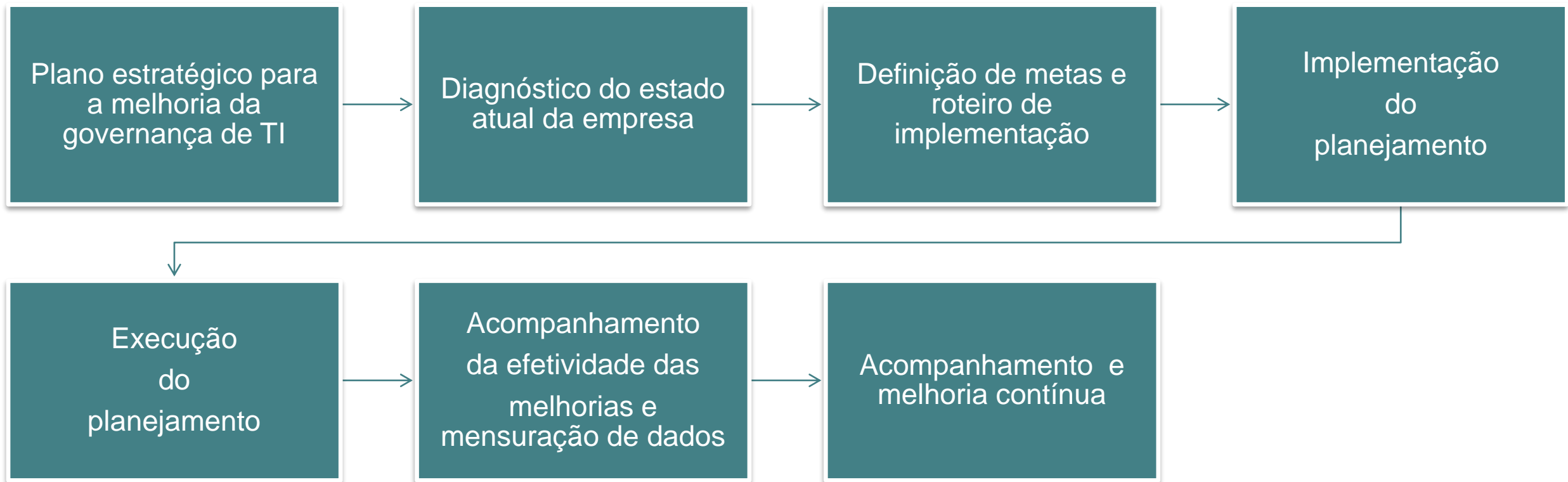
- **Satisfazer as partes interessadas:** A TI deve estar alinhada com todas as áreas da empresa para atender aos objetivos estratégicos de cada setor, beneficiando-se dos serviços de TI e contribuindo para a geração de valor.
- **Cobrir a organização de ponta a ponta:** Todos os processos da empresa são considerados ativos estratégicos, com a gestão de cada setor responsável por gerenciar os processos de TI para atingir os objetivos da organização.



- **Aplicar um framework integrado e único:** Integrar diferentes métodos e frameworks, como ITIL ao COBIT, para criar um único e abrangente framework para a gestão empresarial e de TI.
- **Possibilitar uma visão holística:** Uma visão global da organização é fundamental para a gestão dentro do framework do COBIT.
- **Separar governança e gerenciamento:** Distinguir entre governança de TI e gerenciamento de TI, onde o gerenciamento busca atingir os objetivos da empresa por meio da utilização estratégica de informações, enquanto a governança é a responsabilidade da diretoria ou gestão da empresa para controlar a tecnologia.

No próprio COBIT é possível identificar instruções para a implementação deste framework em 7 etapas, num passo-a-passo didático.

Como implementar o COBIT?




Para saber mais - Vídeo

- **COBIT 5**
 - https://www.youtube.com/watch?v=ML6hU8h8_y8

COSO

- O COSO elaborou um modelo de gestão de riscos corporativos, comumente conhecido como a "Estrutura COSO," com o propósito de auxiliar as organizações na compreensão e na gestão dos riscos críticos para o alcance de seus objetivos.
- A estrutura de gerenciamento de riscos corporativos do COSO é composta por oito componentes interligados que representam a maneira como a administração da organização é conduzida.
- Em outras palavras, o COSO, é um sistema de controle interno que emprega abordagens de avaliação de riscos, embora não tenha sido originalmente concebido como um modelo de gestão de riscos no sentido mais rigoroso.



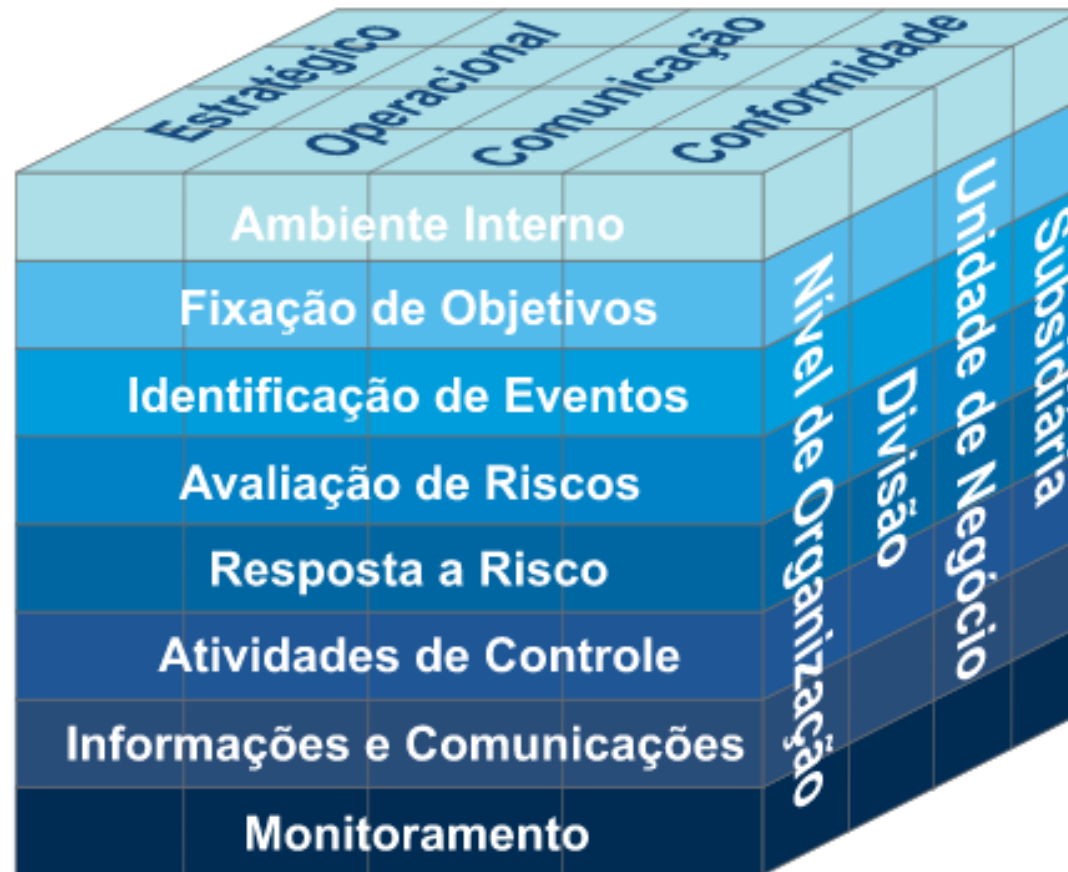
Os componentes do COSO são empregados em diversas áreas da gestão corporativa, abrangendo desde a administração financeira até o gerenciamento de recursos humanos e a governança de TI.

Sua aplicabilidade estende-se a organizações de todos os portes e setores, tanto públicas quanto privadas. Contudo, sua utilização se torna particularmente crítica em setores altamente regulamentados, como o financeiro e o da saúde, nos quais a negligência na gestão de riscos pode resultar em graves implicações legais e impactos na reputação.

A Estrutura COSO representa uma abordagem integrada para o gerenciamento de riscos corporativos e se baseia em três dimensões-chave: objetivos, componentes e unidades organizacionais.

Gerenciamento de Riscos Corporativos

Estrutura Integrada



Objetivos

- A estrutura COSO estabelece quatro categorias de objetivos, que formam o eixo vertical da matriz do COSO:
 - **Objetivos Estratégicos:** são objetivos de alto nível, alinhados com a missão da organização e o plano estratégico global.
 - **Objetivos Operacionais:** são objetivos que se referem à eficácia e eficiência das operações da organização, incluindo o desempenho financeiro e não financeiro.
 - **Objetivos de Comunicação:** se referem à confiabilidade, integridade e precisão dos relatórios da organização.
 - **Objetivos de Conformidade:** se referem ao cumprimento das leis e regulamentos aplicáveis à organização.

Componentes

- Os componentes formam o eixo horizontal da matriz do COSO e são os oito componentes de gerenciamento de riscos corporativos, composta de: ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a riscos, atividades de controle, informações e comunicações e monitoramento.

Ambiente Interno

O ambiente interno exerce influência na forma como a organização percebe e enfrenta os riscos. Neste espaço, a administração estabelece a filosofia de gestão de riscos e define o nível de tolerância ao risco.

Esse contexto é definido pelos traços individuais dos colaboradores, como integridade, valores éticos e competência, além das condições de trabalho em que estão inseridos.

É importante que exista uma clara harmonização entre a cultura organizacional, a estratégia de negócios e a abordagem de gestão de riscos.

Fixação de Objetivos

É o segundo componente fundamental na gestão de riscos. Antes de identificar possíveis riscos, a organização deve possuir objetivos bem definidos.

O gerenciamento de riscos corporativos assegura que a liderança estabeleça um método para a definição dessas metas, garantindo que elas estejam alinhadas com a missão da organização e sejam compatíveis com a sua disposição para lidar com riscos.

Identificação de Eventos

Envolve o reconhecimento de eventos internos e externos que têm o potencial de afetar a consecução dos objetivos da organização.

Esses eventos podem ser categorizados como riscos, oportunidades, ou até mesmo ambos.

As oportunidades são apresentadas à alta administração, que posteriormente formula estratégias ou objetivos em resposta a elas.

Avaliação de Riscos

Após a identificação, os riscos precisam ser submetidos a uma avaliação, levando em conta a probabilidade de ocorrência e os possíveis impactos sobre os objetivos da organização.

A análise de riscos considera tanto os efeitos iniciais quanto os que permanecem.

Essa análise possibilita à gestão uma compreensão mais aprofundada do perfil de risco da organização e, assim, permite a tomada de decisões embasadas sobre a estratégia de gerenciamento a ser adotada.

Resposta a Risco

Responder ao risco inclui identificar e avaliar diferentes maneiras de lidar com ele, como evitar, aceitar, reduzir ou compartilhar o risco.

A administração escolhe a ação mais apropriada para garantir que os riscos estejam alinhados com a capacidade de lidar com riscos e a disposição da organização para enfrentá-los.

Atividades de Controle

- As atividades de controle dizem respeito às políticas e procedimentos estabelecidos para assegurar que as respostas aos riscos escolhidas pela administração sejam implementadas de forma eficaz. Isso envolve a aplicação de medidas internas de controle, como procedimentos operacionais, auditorias internas e restrições de acesso.

Informações e Comunicações

- Um sistema eficaz de informação e comunicação é essencial para a gestão de riscos. Esse sistema assegura que informações relevantes sejam identificadas, coletadas e transmitidas de forma pontual, possibilitando que os colaboradores desempenhem suas funções adequadamente.
- A comunicação eficaz é caracterizada por um fluxo transparente de informações em todas as direções dentro da organização e pela definição clara das funções e responsabilidades dos funcionários.

Monitoramento

- O monitoramento consiste em supervisionar de forma constante o processo de gestão de riscos corporativos e fazer ajustes quando necessário. Através do monitoramento, a organização pode tomar medidas proativas e se ajustar às mudanças nas circunstâncias. Esse acompanhamento é realizado por meio de atividades de gestão contínuas, avaliações independentes ou uma combinação de ambos.

A estrutura do COSO fornece uma abordagem abrangente e integrada para o gerenciamento de riscos corporativos. Adotar e implementar esses componentes da gestão de riscos pode ajudar as organizações a identificar, avaliar e gerenciar efetivamente os riscos, garantindo o alinhamento com seus objetivos estratégicos e a conformidade com as normas regulatórias.

Para saber mais - Vídeo

- **Tudo Sobre o COSO: Controles Internos (COSO ICF) e Gestão de Riscos (COSO ERM)!**
 - <https://www.youtube.com/watch?v=bnov9nv9zGU>