

Gestão de Riscos: Conceitos e Papel da Auditoria Interna

Objetivos

- **Objetivo Geral:** Compreender a gestão de riscos em órgãos e entidades públicas, com vista a ajudar a melhorar a governança pública, bem como entender o papel da auditoria interna em relação ao tema.
- **Objetivos Específicos:**
 - Conhecer os elementos conceituais relacionados à gestão de riscos;
 - Identificar e assimilar as responsabilidades das partes envolvidas na gestão de riscos e controles internos;
 - Conhecer os aspectos gerais de um processo de gestão de riscos;
 - Distinguir os papéis da auditoria interna em relação à gestão de riscos;
 - Explorar estruturas de gestão de riscos;
 - Analisar os normativos sobre a gestão de riscos no Poder Executivo Estadual;
 - Conhecer proposta de implantação de gestão de riscos nas organizações públicas.

Conteúdo Programático

1. **Governança Pública.**
 1. Conceitos. Mecanismos e Estrutura de Governança Pública.
 2. Relação entre governança e gestão.
 3. Mecanismos de Governança Pública.
2. **Fundamentos da gestão de riscos.**
 1. Conceitos. Eventos. Probabilidade e Impacto. Riscos inerentes e residuais. Percepção de Risco. Apetite/Tolerância a riscos. Mitos sobre gestão de riscos.
 2. Categorias e Dicionário de Riscos.
3. **Modelo de Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.**
 1. Papéis e responsabilidades.
 2. Auditoria Interna.
 1. Conceito e papéis em relação à gestão de riscos.

Conteúdo Programático (cont.)



3. Processo de gestão de riscos.
 1. Estabelecimento do Contexto/Ambiente Interno.
 2. Identificação de Riscos.
 3. Avaliação/Análise de Riscos. Cálculo do Risco. Matriz de Risco.
 4. Tratamento/Respostas a Risco. Controles Internos. Avaliação dos Controles Internos.
 5. Informação, Comunicação, Monitoramento e Análise Crítica.
 6. Técnicas/Ferramentas de identificação e análise de riscos.
4. Estruturas de gestão de riscos. COSO e ISO31000. Decreto nº 47.087, de 1º fevereiro de 2019 e Decreto nº 46.855, de 7 de dezembro de 2018, ambos do Estado de Pernambuco.
5. Implantação da gestão de riscos.

Metodologia de Trabalho



- **Metodologia de Ensino:** Leituras comentadas, exposições ativo-participativas do conteúdo, estudos de caso, dramatização, desempenho de papel, discussão sobre vídeos apresentados e exercícios aplicados.
- **Metodologia de Avaliação de Aprendizagem:** Realizada em quatro fases:
 - 1) **diagnóstica** - aplicação de questionário informal com utilização de ferramenta *online* em que se avalia o nível inicial de conhecimentos dos participantes;
 - 2) **formativa** - aplicação de exercícios com utilização de ferramenta *online*;
 - 3) **somativa** - aplicação de questionário informal com utilização de ferramenta *online* em que se verifica em que medida o aprendiz atingiu os objetivos propostos; e
 - 4) **Reação** - aplicação de questionário oficial da(s) escola(s) de governo em que se verifica satisfação após a capacitação e se os elementos do curso (metodologia, instrutor, material etc.) corresponderam às expectativas. Além disso, os participantes serão avaliados por meio de prova do curso de aperfeiçoamento.

Contexto



Conexão	
www.menti.com código: .	• Nome • Organização, departamento, cargo/função • Experiência em gestão de riscos • Expectativa em relação ao curso • Passatempo

Contexto	
POR QUE GESTÃO DE RISCOS?	VUCA • Volatility (Volatilidade): Ritmo elevado com que ocorrem mudanças com impacto nas organizações. • Uncertainty (Incerteza): Quando a informação relevante não está disponível. • Complexity (Complexidade): Diferentes acontecimentos não lineares, interconectados e interdependentes que dificultam a interpretação, dando a sensação de caos. • Ambiguity (Ambiguidade): Quando a informação relevante está disponível, mas o significado geral ainda é desconhecido.

Contexto (continuação)	
AS ORGANIZAÇÕES ESTÃO CONSTANTEMENTE SOB ATAQUE DO MUNDO VUCA!	
Pressão social e política	Desastres naturais
Crises econômicas	Crises energéticas
	Crises de Transporte
Mudança tecnológica	Falha na prestação de serviços...

Contexto (Continuação)



Preceitos para lidar com VUCA

- Visão do todo e não da parte - visão sistêmica;
- Velocidade na tomada de decisão - flexibilidade e coragem;
- Pensar fora da caixa, ser criativo diante das incertezas - inovação;
- Colaboração entre as equipes, redes de colaboração e multidisciplinariedade;
- Agilidade, adaptabilidade e resiliência.

Conclusão...

Um mundo VUCA só pode ser gerenciado com base em riscos.

Dai a importância de todos os gestores saberem e/ou possuírem a competência de lidar com riscos.

Contexto (continuação)



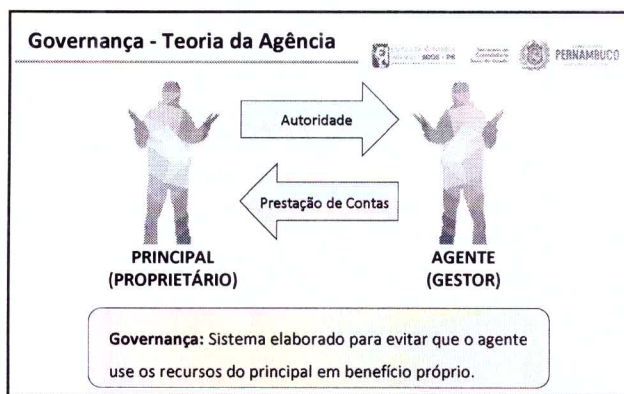
MAIS SOBRE O MUNDO VUCA...



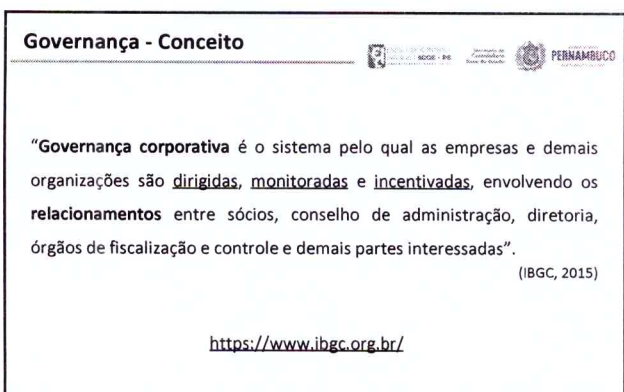
https://www.youtube.com/watch?v=ZuEF76Xs_Mw



Governança Pública

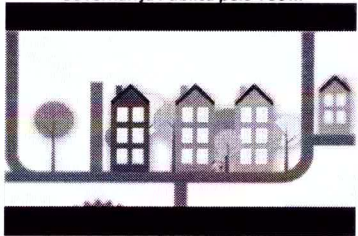






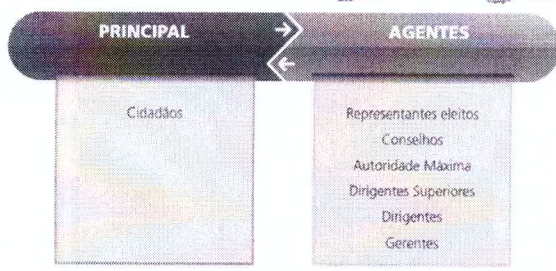
Governança Pública

Governança Pública pelo TCU...



<https://youtu.be/kGYd1mj-0c>

Relação Agente x Principal



Referencial básico de governança aplicável a órgãos e entidades da administração pública (TCU, 2014)

Governança Pública - Conceito

Governança pública é o conjunto de **mecanismos de liderança, estratégia e controle** postos em prática para **avaliar, direcionar e monitorar a gestão**, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade

(Decreto Federal nº 9.203, de 22 de novembro de 2017 e Decreto Estadual nº 46.855, de 7 de dezembro de 2018)

Governança Pública - Sistema



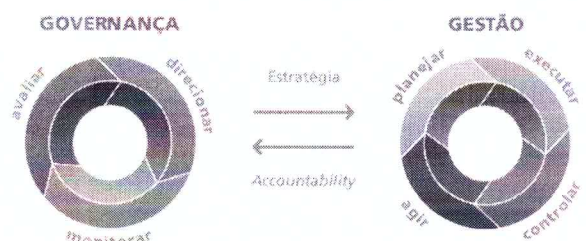
SISTEMA DE GOVERNANÇA PÚBLICA

A maneira como diversos atores se organizam, interagem e procedem para obter boa governança.

- 1) as estruturas administrativas (instâncias);
- 2) os processos de trabalho;
- 3) os instrumentos (ferramentas, documentos, etc);
- 4) o fluxo de informações;
- 5) o comportamento de pessoas envolvidas direta, ou indiretamente, na avaliação, no direcionamento e no monitoramento.

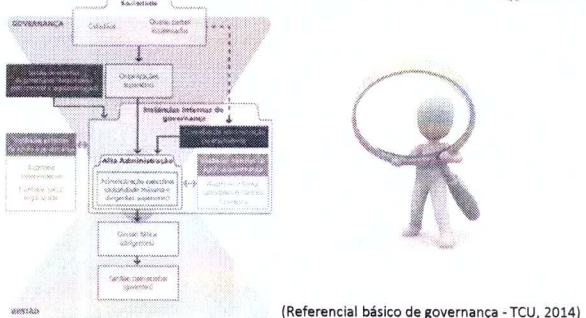
(Referencial básico de governança - TCU, 2014)

Relação Governança x Gestão

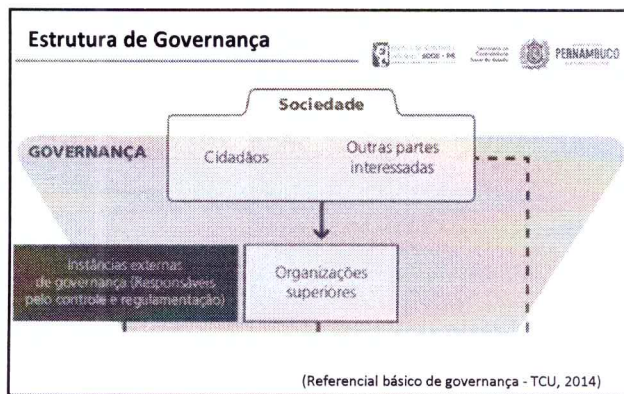


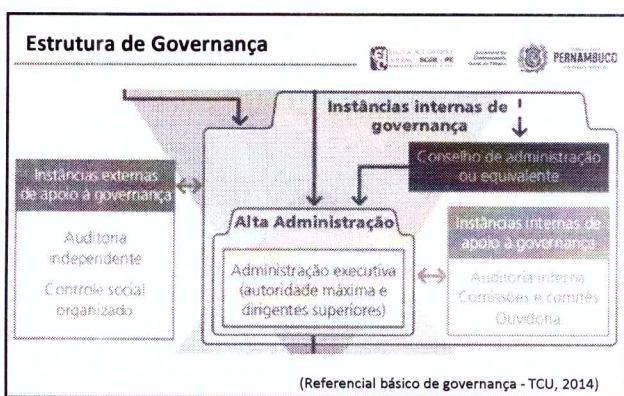
(Referencial básico de governança - TCU, 2014)

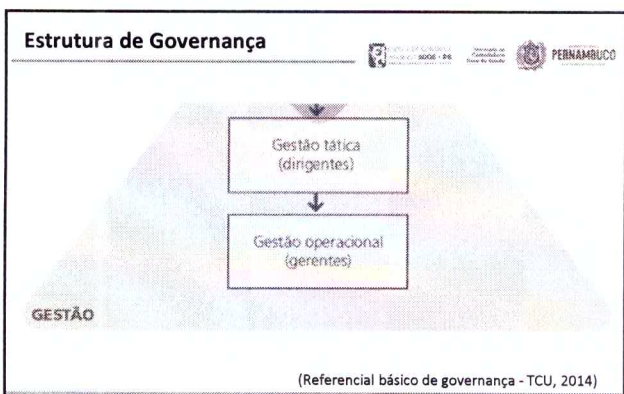
Estrutura de Governança

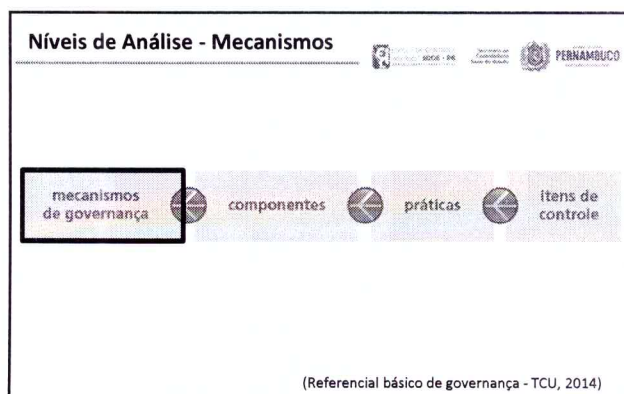


(Referencial básico de governança - TCU, 2014)

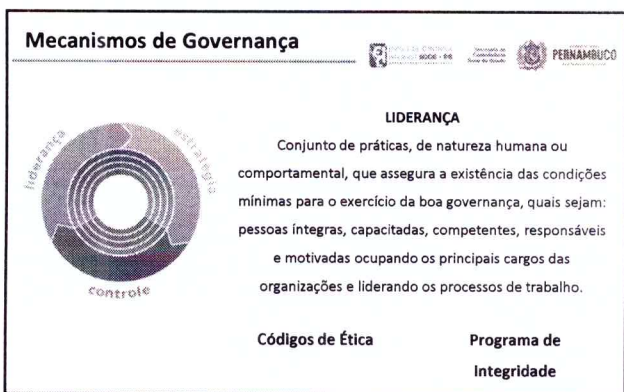












Mecanismos de Governança



ESTRATÉGIA

Envolve aspectos como: escuta ativa de demandas, necessidades e expectativas das partes interessadas; avaliação do ambiente interno e externo da organização; avaliação e prospecção de cenários; definição e alcance da estratégia; definição e monitoramento de objetivos de curto, médio e longo prazo; alinhamento de estratégias e operações das unidades de negócio e organizações envolvidas ou afetadas.

Ouvidoria Planejamento Estratégico

Mecanismos de Governança



CONTROLE

Para que os processos sejam executados, existem riscos, os quais devem ser avaliados e tratados. Para isso, é conveniente o estabelecimento de controles e sua avaliação, transparência e accountability, que envolve, entre outras coisas, a prestação de contas das ações e a responsabilização pelos atos praticados.

Gestão de Riscos Transparência Correição

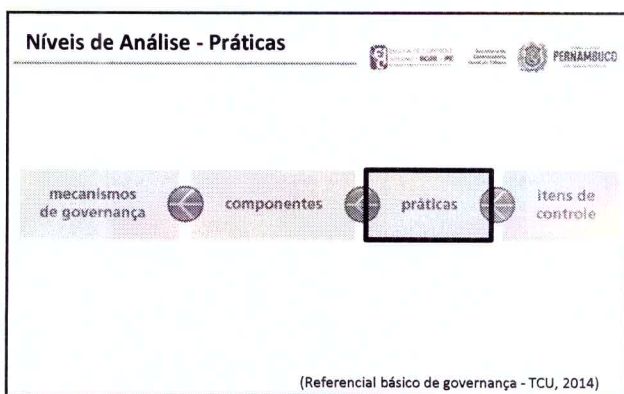
Auditoria Interna Prestação de Contas

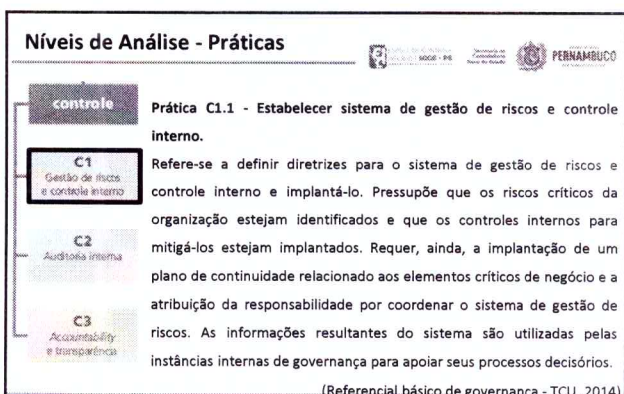
Níveis de Análise - Componentes



(Referencial básico de governança - TCU, 2014)







Níveis de Análise - Práticas

controle

C1
Gestão de riscos e controle interno

C2
Auditoria interna

C3
Accountability e transparência

Prática C1.2 - Monitorar e avaliar o sistema de gestão de riscos e controle interno, a fim de assegurar que seja eficaz e contribua para a melhoria do desempenho organizacional.

Pressupõe que o sistema de gestão de riscos e controle interno seja monitorado e avaliado pela mais alta instância interna de governança da organização, considerando aspectos como conformidade legal e regulamentar, aderência a boas práticas, alinhamento a estratégias da organização e desempenho global.

Como resultado do monitoramento e avaliação, medidas visando o aprimoramento do sistema são implementadas sempre que necessário.

(Referencial básico de governança - TCU, 2014)

Níveis de Análise - Práticas

controle

C1
Gestão de riscos e controle interno

C2
Auditoria interna

C3
Accountability e transparência

Prática C2.1 - Estabelecer a função de auditoria interna.

Envolve definir o propósito, autoridade e responsabilidade da auditoria interna em estatuto que estabeleça a sua posição dentro da organização, autorize acesso aos recursos organizacionais necessários ao desempenho dos seus trabalhos e defina o escopo de suas atividades. Implica, ainda, a implantação da função de auditoria, resultando na produção de relatórios relevantes destinados às instâncias internas de governança.

(Referencial básico de governança - TCU, 2014)

Níveis de Análise - Práticas

controle

C1
Gestão de riscos e controle interno

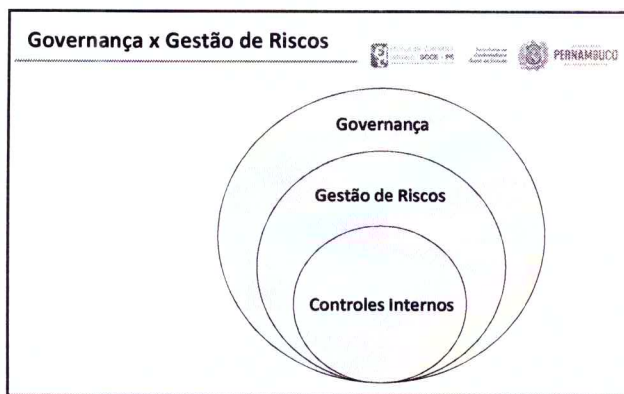
C2
Auditoria interna

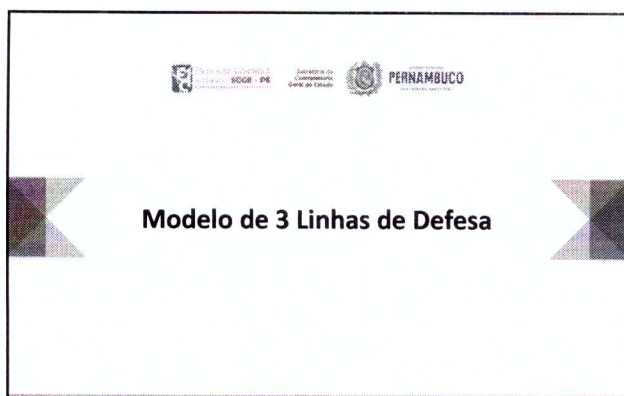
C3
Accountability e transparência

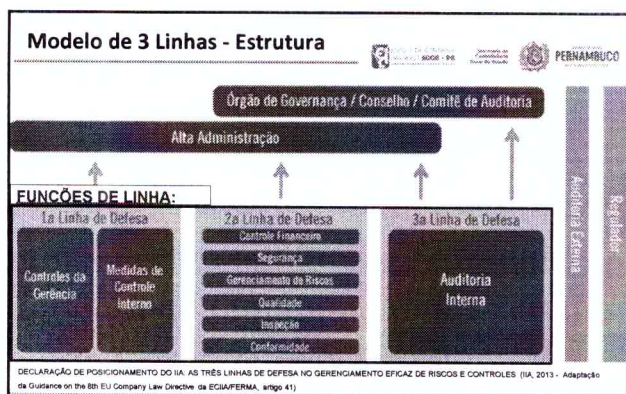
Prática C2.2 - Prover condições para que a auditoria interna seja independente e proficiente.

Requer que a auditoria interna se reporte funcionalmente à mais alta instância interna de governança e, administrativamente, à alta administração. Envolve, ainda, definir diretrizes para o tratamento de conflitos de interesse na função de auditoria interna e identificar competências necessárias ao desempenho de suas responsabilidades, provendo condições para que os auditores internos possuam, coletivamente, as competências identificadas.

(Referencial básico de governança - TCU, 2014)



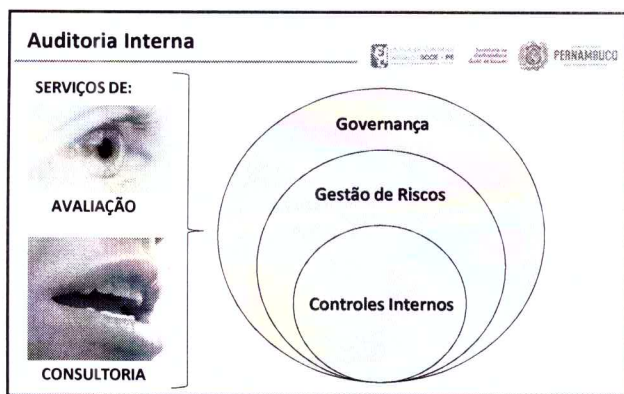


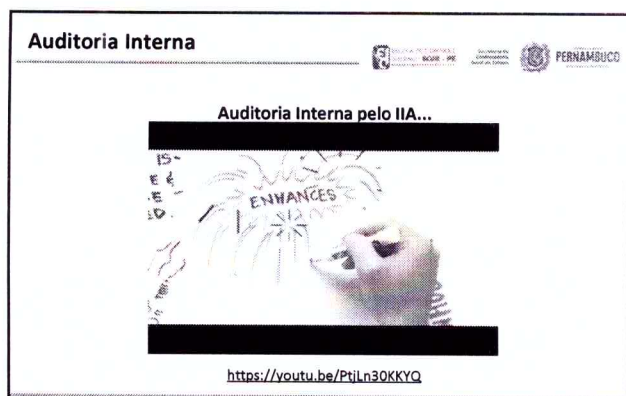


Modelo de 3 Linhas - Funções		
1ª LINHA	2ª LINHA	3ª LINHA
Gestão Operacional. Responsável por gerenciar os riscos e tem propriedade sobre eles, devendo implementar as ações corretivas para resolver deficiências em processos e controles.	Constituída por funções (unidades, comitês ou outras estruturas organizacionais). Ex.: Comitê de Risco. Estabelecidas para auxiliar a desenvolver e/ou monitorar os controles da primeira linha de defesa.	Auditoria Interna. Fornecer avaliações e consultoria sobre os processos de governança, gestão de riscos, controles internos aos órgãos de governança e à alta administração da organização.

Modelo de 3 Linhas
Órgãos de governança (Conselho de Administração e equivalentes) e a alta administração • Não são considerados dentre as três "linhas" do modelo, mas são as principais partes interessadas atendidas pelas "linhas" e são as partes em melhor posição para ajudar a garantir que o modelo seja aplicado. • Têm, coletivamente, a responsabilidade e o dever de prestação de contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançar esses objetivos e o estabelecimento de estruturas e processos de governança para melhor gerenciar os riscos durante a realização desses objetivos. • O modelo de Três Linhas de Defesa é implementado melhor com o apoio ativo e a orientação do órgão de governança e da alta administração da organização. DECLARAÇÃO DE POSICIONAMENTO DO IIA, AS TRÊS LINHAS DE DEFESA NO GERENCIAMENTO EFICAZ DE RISCOS E CONTROLES, JUL. 2013

Auditoria Interna
A auditoria interna é uma atividade independente e objetiva de avaliação e consultoria, criada para agregar valor e melhorar as operações de uma organização. Ela auxilia a organização a atingir seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada à avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, controle e governança. A auditoria interna representa a terceira linha no Modelo de 3 Linhas de Defesa. Possui o maior nível de independência e objetividade dentro da organização. A auditoria interna avalia, presta consultoria e pode defender a implantação da gestão de riscos e controles, mas não deve implantá-los, visto que comprometeria a independência e objetividade na prestação de serviço à organização.







Gestão de Riscos

Gestão de Riscos pelo TCU...

**MAS AFINAL,
O QUE É UM RISCO??**

https://youtu.be/SOKSrIOS_4

Riscos - Conceitos

- A possibilidade de que um evento ocorra e afete negativamente a realização dos objetivos (COSO)
- **Efeito da incerteza nos objetivos.** O efeito é um desvio em relação ao esperado, podendo ser positivo e/ou negativo (ISO 31000)

"Situação específica em um determinado momento futuro que, devido à natureza do negócio naquele momento, é de particular interesse para você".

(<https://www.strategic-risk-europe.com/why-current-risk-definitions-just-dont->

Elementos Associados aos Riscos

- **Objetivos:** Resultados que se pretende atingir.
- **Evento:** Incidente ou ocorrência de fontes internas ou externas a uma organização, que podem afetar a consecução dos objetivos. Os eventos podem ter impacto negativo, impacto positivo ou ambos.
- **Impacto:** Efeito do evento.
- **Probabilidade:** Possibilidade do evento.
- **Percepção de risco:** Julgamento subjetivo sobre probabilidade e/ou impacto de um evento. É influenciada por condições psicossociais (emoções, vida pessoal, etc.), fisiológicas (Saúde do corpo, alimentação, remédios, etc.) e cognitivas (conhecimento sobre o setor e as tarefas).

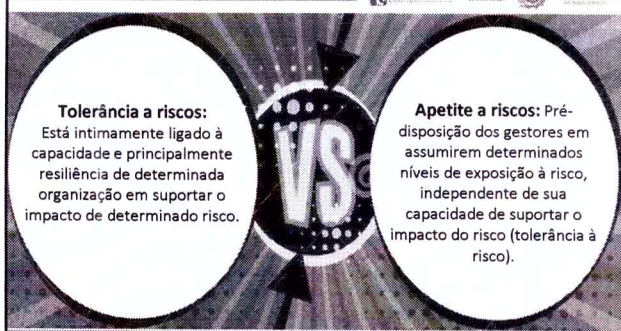
Problema x Risco



PROBLEMA: uma situação ou condição existente que afeta no momento presente os objetivos e que requer uma solução.

Um risco, quando se concretiza, torna-se uma problema.

Tolerância x Appetite



Inerente x Residual



- Risco inerente é o nível de risco antes de quaisquer ações de mitigação de risco terem sido levadas em conta, como atividades de controle, também chamados de controles internos. Exemplo: o risco inerente de inundação antes de levar em consideração as medidas de prevenção de inundações.
- Risco residual é o nível de risco após ter levado em consideração as ações de mitigação de risco tais como controles internos. As áreas que são bem controladas geralmente terão níveis mais baixos de risco residual.

Inerente x Residual (continuação)



RISCO INERENTE

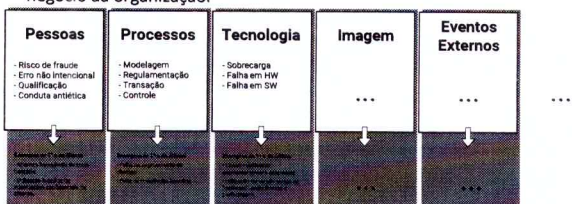
- ATIVIDADES DE CONTROLE

RISCO RESIDUAL

Dicionário de Riscos



- O dicionário de riscos serve para classificar/categorizar os riscos em uma linguagem comum, considerando as características e o ambiente de negócio da organização.



Crouhy et al(2001, p. 475, apud Trapp, 2004, p. 50)

Gestão de Riscos - Conceito



Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

(DECRETO FEDERAL Nº 9.203, DE 22 DE NOVEMBRO DE 2017 e
DECRETO ESTADUAL Nº 46.855, DE 7 DE DEZEMBRO DE 2018)

Gestão de Riscos

Para que serve Gestão de Riscos?



<https://www.youtube.com/watch?v=ZFhgIqX5e7E>

Gestão de Riscos - Mitos

- Complexo
- Burocrático
- Eleva os custos
- Necessita de consultorias
- Somente com sistemas



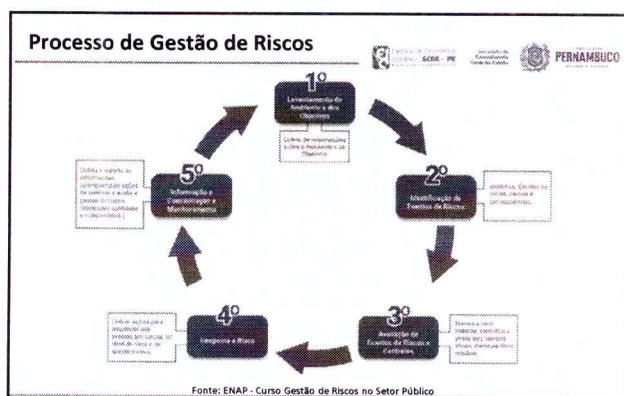
Gestão de Riscos

Por que Gestão de Riscos?



https://youtu.be/_n15QnZnJc





Processo de Gestão de Riscos

**Levantamento do Ambiente Interno e Objetivos
(Estabelecimento do Contexto)**

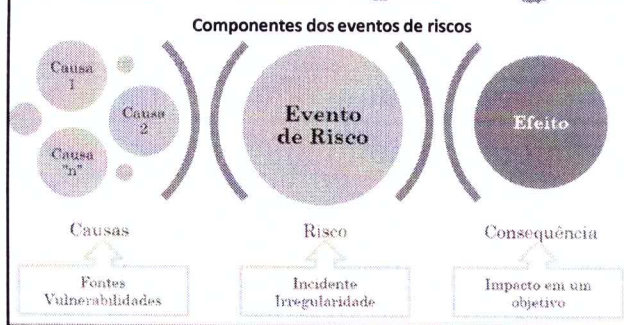
- O levantamento do ambiente interno e dos objetivos é a etapa do processo de gestão de riscos que envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas;
- Os objetivos são a essência da definição do contexto, pois a gestão de riscos ocorre

Identificação de Riscos

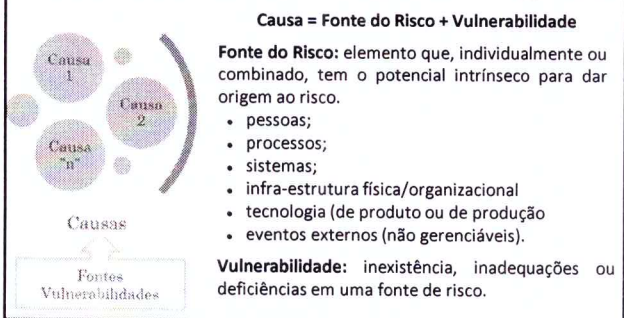


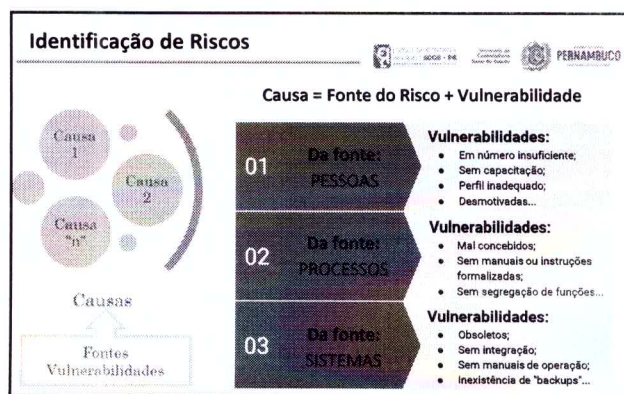
Processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e apoiando-se na comunicação e consulta com as partes interessadas internas e externas (ABNT, 2009).

Identificação de Riscos



Identificação de Riscos





Identificação de Riscos

Sintaxe de descrição dos eventos de riscos

Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS> impactando no/na <OBJETIVO DE PROCESSO>.

DICAS

- Sempre relacionado aos objetivos;
- Evitar descrever o impacto como próprio risco;
- Evitar descrever riscos que não impactam os objetivos;
- Evitar descrever risco como o oposto do objetivo;
- Deve incluir causa e consequência;
- Riscos podem ser agrupados.

Fonte: Orange Book

Identificação de Riscos

TÉCNICAS

- Questionários - Lista de Verificação (Checklist) - Workshop - Brainstorming - Inspecções/auditorias - Mapeamento de Processos	- Método Delphi - Fluxogramas - Diagrama de causa e efeito - Bow-tie; - Método dos 5 porquês - Etc.
--	--

Identificação de Riscos

Identificação de Riscos x Mapeamento de Processos

Embora seja uma boa prática de gestão, o mapeamento dos processos não é essencial para a gestão de riscos, sendo necessária a identificação dos processos.

Avaliação/Análise de Riscos

Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e/ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido (ABNT, 2009).

Auxilia na tomada de decisões, em especial: (a) se um determinado risco precisa de tratamento e a prioridade para isso; (b) se uma determinada atividade deve ser realizada ou descontinuada; e (c) se controles internos devem ser implementados ou, se já existirem, se devem ser modificados, mantidos ou eliminados.

Avaliação/Análise de Riscos

Nível de Risco = Função (Probabilidade, Impacto)

Nível de Risco = Probabilidade x Impacto

Nível de Risco = Probabilidade^a x Impacto^b

Avaliação/Análise de Riscos		
		
ESCALA DE PROBABILIDADE (EXEMPLO)		
PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Avaliação/Análise de Riscos		
		
ESCALA DE IMPACTO (EXEMPLO)		
IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Avaliação/Análise de Riscos			
			
ESCALA DE IMPACTO (EXEMPLO 2)			
Gravidade do Evento ou Problema	Falta na entrega de um produto operacional	Falta na entrega de um produto administrativo	Falta na entrega de um produto estratégico
Problema	Impacto financeiro que excede o valor de R\$ 500.000,00.	Impacto financeiro significativo que excede o valor de R\$ 250.000,00, representando a perda de R\$ 10.000,00.	Impacto financeiro significativo que excede o valor de R\$ 100.000,00, representando a perda de R\$ 5.000,00.
Problema Operacional	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.
Calor de Impacto	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.
Repercussão Social	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.
Prejuízo	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.	Impacto e perda de produtividade operacional no âmbito da organização.
	1	2	3
	Baixo	Baixo	Baixo

Avaliação/Análise de Riscos

GOV. DO PERNAMBUCO
SECRETARIA DE GOVERNO
SECRETARIA DE SEGURANÇA PÚBLICA

ESCALA DE IMPACTO (EXEMPLO 3)

Impacto: Escala para a Avaliação

Categorias de Impacto	Escala de Impacto					Nível de Impacto
	1%	2%	3%	4%	5%	
Condições para avaliação de risco	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema
	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema
	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema
	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema
	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema	Impacto com consequências graves para a segurança ou integridade do sistema

Avaliação/Análise de Riscos

GOV. DO PERNAMBUCO
SECRETARIA DE GOVERNO
SECRETARIA DE SEGURANÇA PÚBLICA

ESCALA DE NÍVEL DE RISCO (EXEMPLO)

RM (Risco Médio)	RA (Risco Alto)	80 - 100
0 - 9,99	10 - 39,99	40 - 79,99
Muito Baixa	Baixa	Média
1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16	17	18
19	20	21
22	23	24
25	26	27
28	29	30
31	32	33
34	35	36
37	38	39
40	41	42
43	44	45
46	47	48
49	50	51
52	53	54
55	56	57
58	59	60
61	62	63
64	65	66
67	68	69
70	71	72
73	74	75
76	77	78
79	80	81
82	83	84
85	86	87
88	89	90
91	92	93
94	95	96
97	98	99
100	101	102

MATRIZ DE RISCO:

Técnica/ferramenta de Análise de Risco

Avaliação/Análise de Riscos

GOV. DO PERNAMBUCO
SECRETARIA DE GOVERNO
SECRETARIA DE SEGURANÇA PÚBLICA

AValiação dos Riscos Inerentes

AValiação de Controles

AValiação dos Riscos Residuais

Nível de risco inerente (NRI) é o nível de risco antes da consideração das respostas que a Administração adota para reduzir a probabilidade (P) do evento ou os seus impactos (I) nos objetivos, incluindo controles internos.

Nível de Confiança (NC) forma de avaliar o efeito dos controles internos na mitigação de riscos mediante análise dos atributos do desenho e da implementação do controle.

Risco de controle (RC) possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência eventos que possam afetar adversamente a realização de objetivos.

Nível de risco residual (NRR), o risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações.

NRI = P x I

RC = 1 - NC

NRR = NRI x RC

Avaliação/Análise de Riscos		
NÍVEL DE CONFIANÇA (NC)	AValiação do Desenho e Implementação dos Controles (ATRIBUTOS DO CONTROLE)	RISCO DE CONTROLE (RC)
Insuficiente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1,0
Fraco NC = 70% (0,7)	Controles têm abrangência, mas tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Alto 0,8
Mediano NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

NÃO EXISTE RISCO ZERO! RISCOS NÃO SÃO ELIMINADOS!

Avaliação/Análise de Riscos			
RISCOS IDENTIFICADOS	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO INERENTE (NRI)
Risco 1 - Descrição do risco 1	Alto - 8	Muito Alto - 10	80 RM (Alto)
Risco 2 - Descrição do risco 2	Médio - 5	Alto - 8	40 RM (Alto)
Risco 3 - Descrição do risco 3	Baixa - 2	Médio - 5	10 RM (Médio)
Risco n - Descrição do risco n	Muito Baixa - 1	Muito Baixa - 5	5 RM (Baixo)

RISCOS IDENTIFICADOS	P	I	NÍVEL DE RISCO INERENTE (NRI)	EFICIÊNCIA DO CONTROLE	RISCO DE CONTROLE (RC)	NÍVEL DE RISCO RESIDUAL (NRR)	NÍVEL DE CONFIANÇA (NCC)
Risco 1	Alto - 8	M. Alto - 10	80	Inexistente	1,0	80	0% (0,0)
Risco 2	Médio - 5	Alto - 8	40	Mediano	0,6	24	40% (0,4)
Risco 3	Baixa - 2	Alto - 5	10	Fraco	0,8	8	20% (0,2)

RC = 1 - NC NRR = NRI x RC

Avaliação/Análise de Riscos	
Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento associados aos níveis de risco. Exemplo:	
NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS
EL	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.
RA	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
RM	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
AB	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Resposta/Tratamento de Riscos



O tratamento de riscos envolve a seleção de uma ou mais alternativas para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes.

(ABNT, 2009; COSO, 2006)

Resposta/Tratamento de Riscos



Informação/Comunicação/Consulta



Durante todas as etapas deve haver comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para:

- Auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;
- Auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização; e
- garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos.

Convém que seja desenvolvido um plano de comunicação e realizada consulta interna e externa para apoiar essa atividade, seja por meio de documento formal ou de lista de verificação.

Monitoramento e Análise Crítica



Tem por finalidade:

- detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes;
- obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;
- analisar eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; e
- assegurar que os controles sejam eficazes e eficientes no projeto e na operação

(ABNT, 2009).

Monitoramento e Análise Crítica

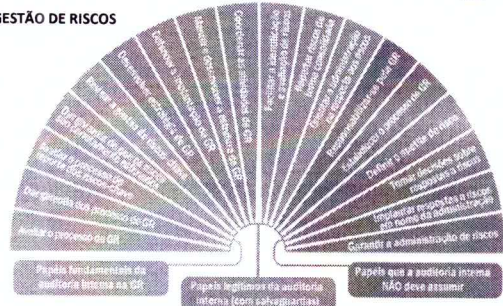


- Monitoramento contínuo** (ou pelo menos, frequente) pelas funções que gerenciam e têm propriedade de riscos e pelas funções que supervisionam riscos;
- Análise crítica dos riscos** e seus tratamentos realizada pelas funções que gerenciam e têm propriedade de riscos e/ou pelas funções que supervisionam riscos, por meio de **autoavaliação de riscos e controles** (Control and Risk Self Assessment - CRSA);
- Auditorias** realizadas pelas funções que fornecem avaliações independentes, seja por meio de auditoria interna ou externa, focando na estrutura e no processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez de situações específicas.

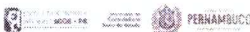
Papéis da Auditoria Interna



GR = GESTÃO DE RISCOS



Avaliação de Aprendizagem



www.menti.com
Código:

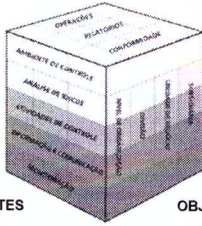


Estruturas de Gestão de Riscos

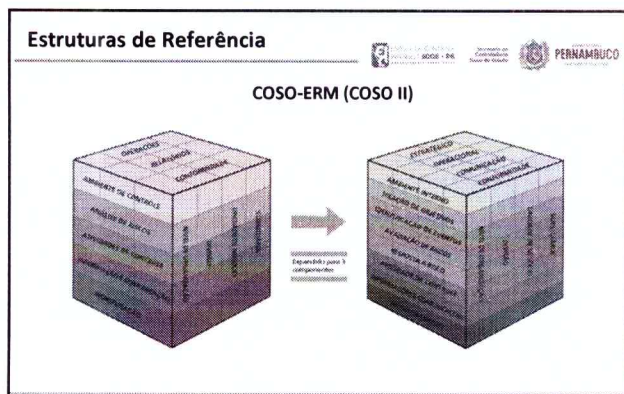
Estruturas de Referência

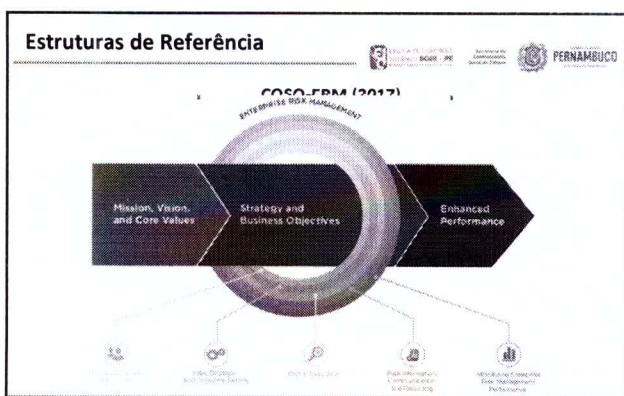


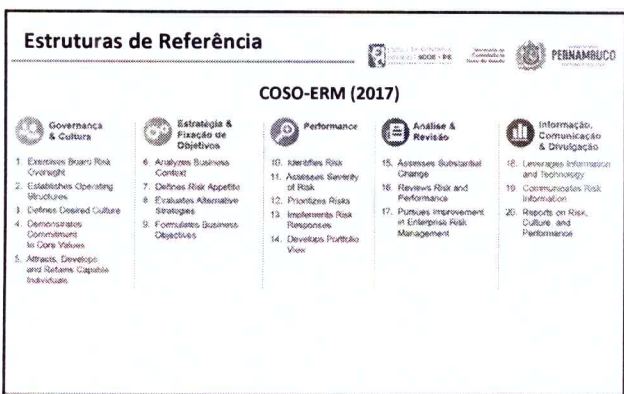
COSO-ICIF (COSO I)
OBJETIVOS

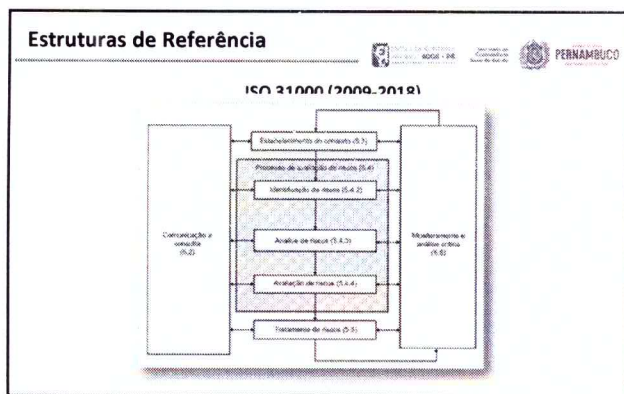


COMONENTES **OBJETOS DE CONTROL**









Estrutura Estadual

Decreto nº 47.087, de 1º fevereiro de 2019

Decreto nº 46.855, de 7 de dezembro de 2018

Decreto nº 47.087/2019

DECRETO Nº 47.087/2019 (Setoriais de Controle Interno) Art. 4º [...] Parágrafo único, As Setoriais de Controle Interno - SCIs são responsáveis por proceder à avaliação e supervisão do gerenciamento de riscos e da operacionalização dos controles internos executados por todos os níveis de gestão dentro da organização. Art. 6º A Setorial de Controle Interno - SCI compete: 1 - avaliar os procedimentos de controle e gerenciamento de riscos adotados pelas unidades organizacionais do órgão ou entidade, por meio de auditoria interna, propondo medidas corretivas quando os mesmos forem inexistentes ou se revelarem vulneráveis;	DECRETO Nº 47.087, DE 1º FEVEREIRO DE 2019 (Unidades de Controle Interno) CONSIDERANDO o modelo das Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles do Institute of Internal Auditors - IIA; CONSIDERANDO a necessidade de identificar os riscos, estabelecer controles organizacionais e aumentar a eficácia dos sistemas de gerenciamento respectivos; Art. 2º A Unidade de Controle Interno será instância interna de governança do órgão ou da entidade onde for instituída.
---	---

Decreto nº 46.855/2018

Art. 4º São **diretrizes** da governança pública:

[...]

VI - **implementar controles internos fundamentados na gestão de risco**, que privilegiará ações estratégicas de prevenção a processos sancionadores;

Art. 5º São **mecanismos** para o exercício da governança pública:

[...]

III - **controle**, que compreende processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos.

Decreto nº 46.855/2018

Art. 17. A **alta administração** das organizações da administração pública estadual direta, autárquica e fundacional **deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos** com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios:

I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II - integração da **gestão de riscos** ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III - estabelecimento de controles internos proporcionais aos **riscos**, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

Decreto nº 46.855/2018

Art. 17. [...] V - utilização dos resultados da **gestão de riscos** para apoio à melhoria contínua do desempenho e dos processos de **gerenciamento de risco**, controle e governança.

Art. 18. A auditoria interna governamental deverá adicionar valor e melhorar as operações das organizações para o alcance de seus objetivos, mediante a abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de **gerenciamento de riscos**, dos controles e da governança, por meio de:

I - realização de trabalhos de avaliação e consultoria de forma independente, segundo os padrões de auditoria e ética profissional reconhecidos internacionalmente;

II - adoção de abordagem baseada em **risco** para o planejamento de suas atividades e para a definição do escopo, da natureza, da época e da extensão dos procedimentos de auditoria;

Decreto nº 46.855/2018

Art. 19. Os órgãos e as entidades da administração direta, autárquica e fundacional instituirão programa de integridade, com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção, estruturado nos seguintes eixos:

- I - comprometimento e apoio da alta administração;
- II - existência de unidade responsável pela implementação no órgão ou na entidade;
- III - análise, avaliação e gestão dos riscos associados ao tema da integridade; e
- IV - monitoramento contínuo dos atributos do programa de integridade.

Implantação da gestão de riscos**Passos para implantação:**

- Passo 01:** Decida gerenciar riscos de forma proativa
- Passo 02:** Aprenda sobre gestão de riscos
- Passo 03:** Defina papéis e responsabilidades
- Passo 04:** Estabeleça a política de gestão de riscos
- Passo 05:** Defina o processo de gestão de riscos
- Passo 06:** Identifique os riscos-chave
- Passo 07:** Trate e monitore os riscos-chave
- Passo 08:** Mantenha canais de comunicação com as partes interessadas
- Passo 09:** Incorpore a gestão de riscos aos processos organizacionais
- Passo 10:** Avalie e aprimore a gestão de riscos

10 passos para a boa gestão de riscos (TCU, 2018)

