Diagnóstico de MATURIDADE EM RISCOS

Versão Jan/2026

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

Gestão de Riscos
SCGE-PE

SUMÁRIO

01 CONCEITOS

1.1. O QUE É RISCOS?

Possibilidade de que eventos venham a ocorrer e ***afetem o alcance da estratégia e dos objetivos do negócio.***

~COSO ERM 2017

1.2. O QUE É GESTÃO DE RISCOS?

"Existem duas maneiras de lidar com riscos:

i. ***ser surpreendido*** *por eventos que podem impactar adversamente o alcance dos objetivos da organização e então* ***reagir a eles****, o que caracteriza a cultura de* ***"apagar incêndios"****;*

ii. ou ***antecipar-se a eles****, adotando medidas conscientes que mantenham ou reduzam a probabilidade ou o impacto dos eventos nos objetivos.*

Apenas a segunda maneira pode ser chamada de gestão de riscos*"*

~TCU 2017

1.3. DESAFIO

Riscos e controles sempre andaram juntos:

Art. 14. O trabalho administrativo será racionalizado mediante simplificação de processos e supressão de contrôles que se evidenciarem como puramente formais ou cujo custo seja evidentemente superior ao risco.

~ Decreto-Lei 200/1967

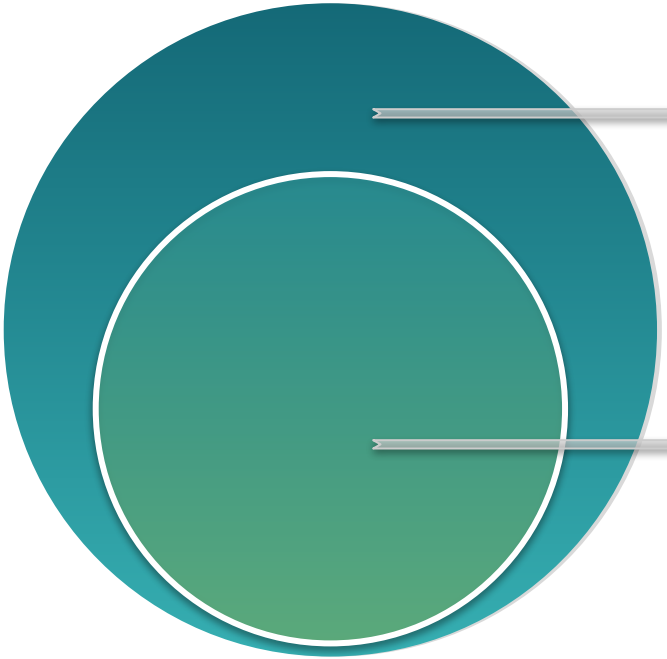
* Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências.

1.4. GESTÃO E GERENCIAMENTO DE RISCOS

1. São elaborados **Mapas de Riscos** de temas diversos?
2. As **ações** de tratamento de riscos são **implementadas**?

1. Os resultados do **monitoramento** são apresentados regularmente à alta gestão? Com qual frequência?
2. Como são **comunicados** os riscos e as estratégias de mitigação às partes interessadas internas e externas?
3. Existem **incentivos ou reconhecimento** para equipes que adotam boas práticas de gestão de riscos?
4. Há **alocação adequada de recursos** (financeiros, humanos e tecnológicos) para implementar a gestão de riscos?
5. Existe **integração** entre o sistema de monitoramento de riscos e outros sistemas de gestão do órgão?

1.4. GESTÃO E GERENCIAMENTO DE RISCOS



GESTÃO DE RISCOS

Aplicação sistemática de Políticas, Procedimentos e Práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos - ISO Guia 73:2009

GERENCIAMENTO DE RISCOS

Processo de identificação, avaliação e resposta aos riscos, compreendendo desde as etapas de definição de contexto e escopo até a elaboração do plano de tratamento

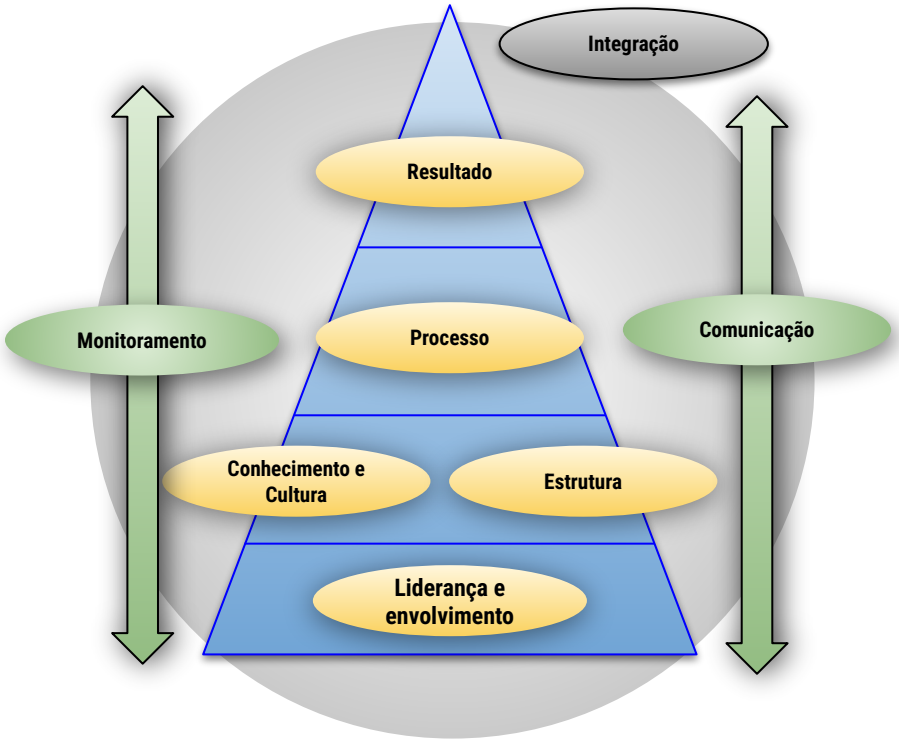
1.5. O QUE É MATURIDADE?

Maturidade de risco é uma medida de **quão bem uma organização identifica, avalia, gerencia e monitora riscos.**

Ela se refere ao nível de qualidade e integração das práticas de gestão de risco de uma organização.

02 MODELO SUGERIDO

2.1 VISÃO GERAL



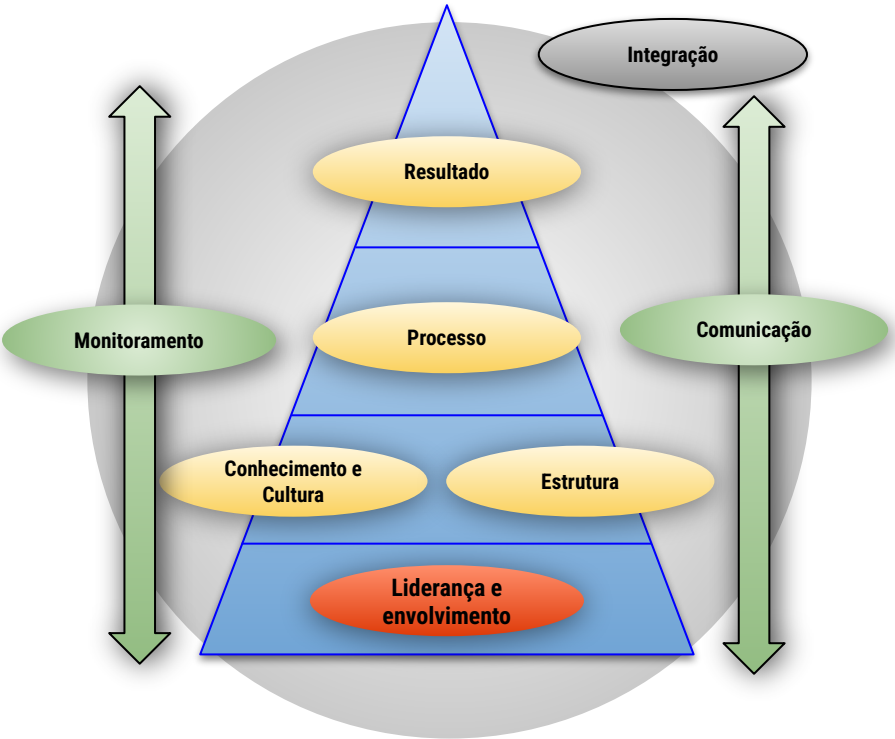
24 práticas, divididas de acordo com a metodologia sugerida pela SCGE-PE

Autoavaliação da UCI

Respostas simples e Diretas

Formulário de Maturidade

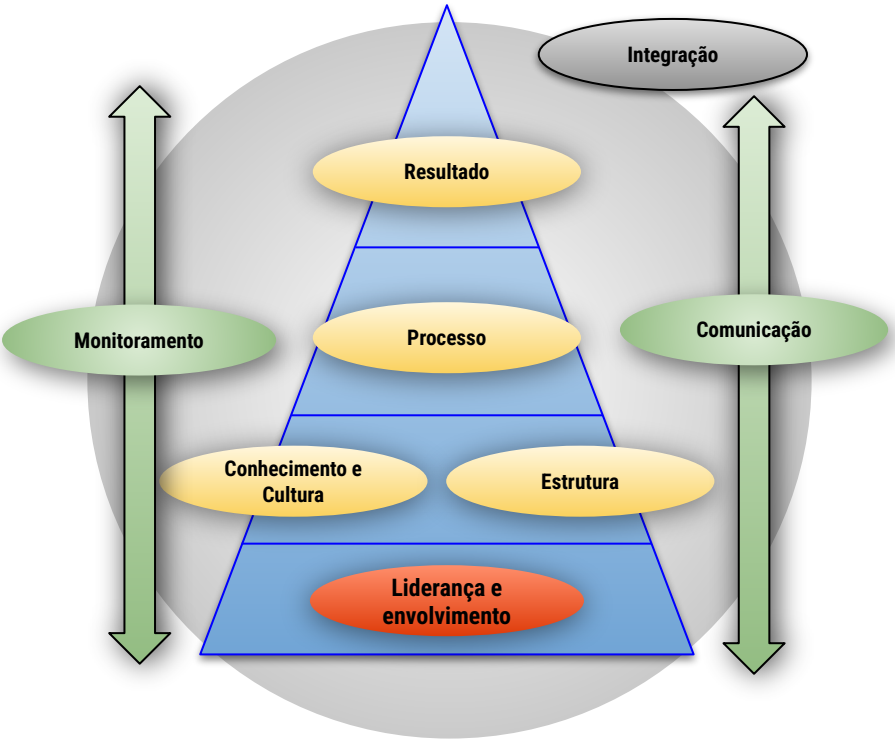
2.2 LIDERANÇA E ENVOLVIMENTO



CONCEITO

Quando a alta administração demonstra um compromisso claro com a gestão de riscos, definindo diretrizes estratégicas e se envolvendo ativamente no processo de gerenciamento de riscos estratégicos, cria-se um ambiente onde a gestão de riscos é priorizada e valorizada em todos os níveis da organização.

2.2 LIDERANÇA E ENVOLVIMENTO

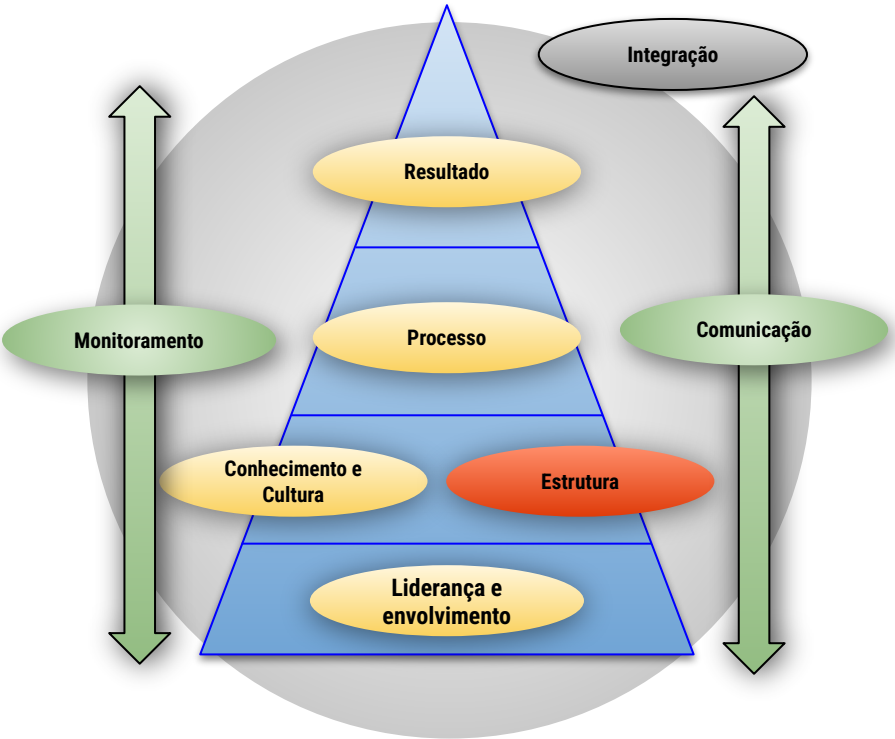


REQUISITOS

1.Existe **diretriz estratégica** para assegurar que o gerenciamento de riscos seja realizado nos PRINCIPAIS níveis hierárquicos do órgão/entidade.

2. O **Gerenciamento dos Riscos Estratégicos** é implementado no órgão/entidade.

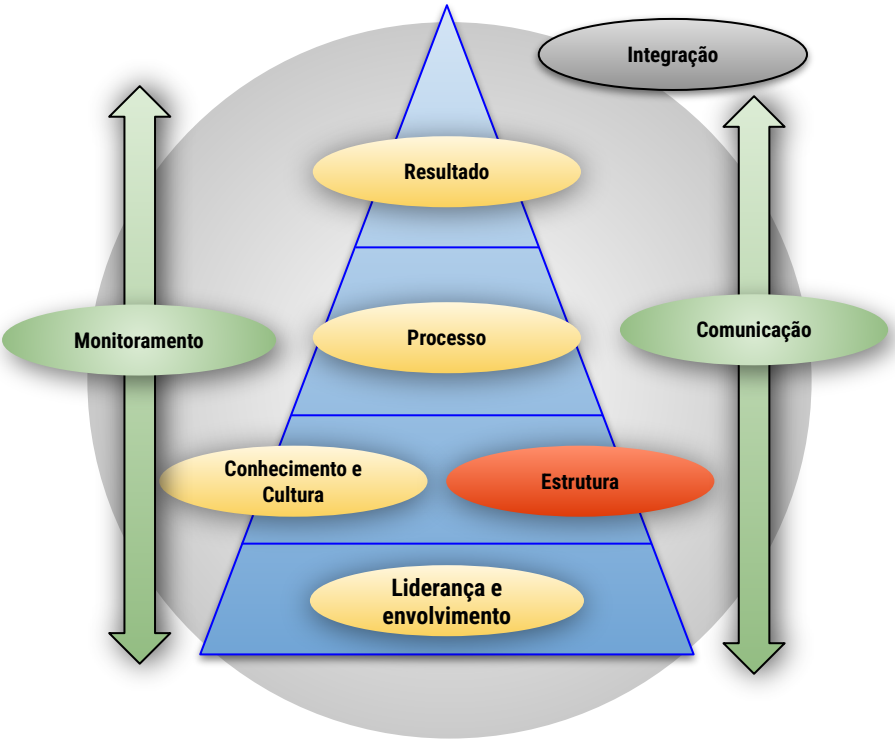
2.4. ESTRUTURA



CONCEITO

Refere-se aos alicerces necessários para desenvolvimento eficaz e regular do processo de Gestão de Riscos. Este grupo traz práticas de planejamento estratégico, de definição de metas e indicadores, e do uso de sistemas informatizados para gerenciar e monitorar riscos. Também aborda a importância da existência de uma política formal de gestão de riscos aprovada e comunicada.

2.4. ESTRUTURA



REQUISITOS

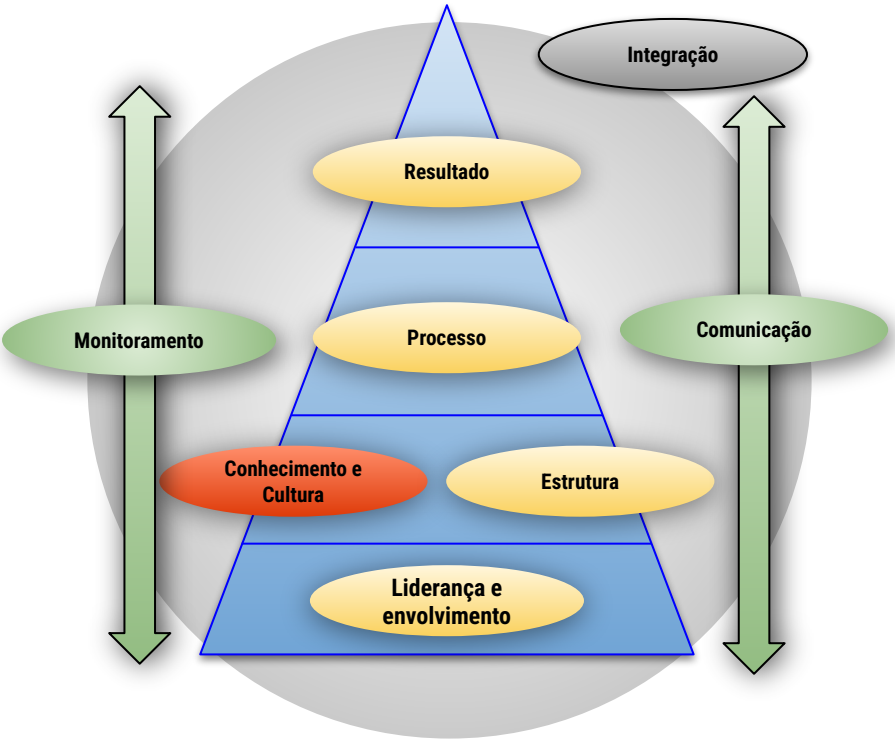
3. O órgão/entidade possui planejamento estratégico (atualizado) contendo, dentre outras informações indispensáveis, as definições de missão, visão e objetivos.

4. O órgão/entidade estabeleceu e comunicou adequadamente **metas** e **indicadores** dos projetos e processos para monitorar seu **desempenho**.

5. Os dados do gerenciamento de riscos são processados através de **sistema informatizado** que permite uma visão abrangente dos riscos da organização e a manutenção do histórico das análises realizadas.

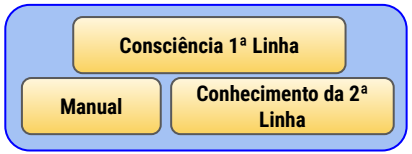
6. O órgão/entidade dispõe de uma **política de gestão de riscos** aprovada pela alta administração, comunicada e disponível às partes interessadas.

2.3 CONHECIMENTO E CULTURA

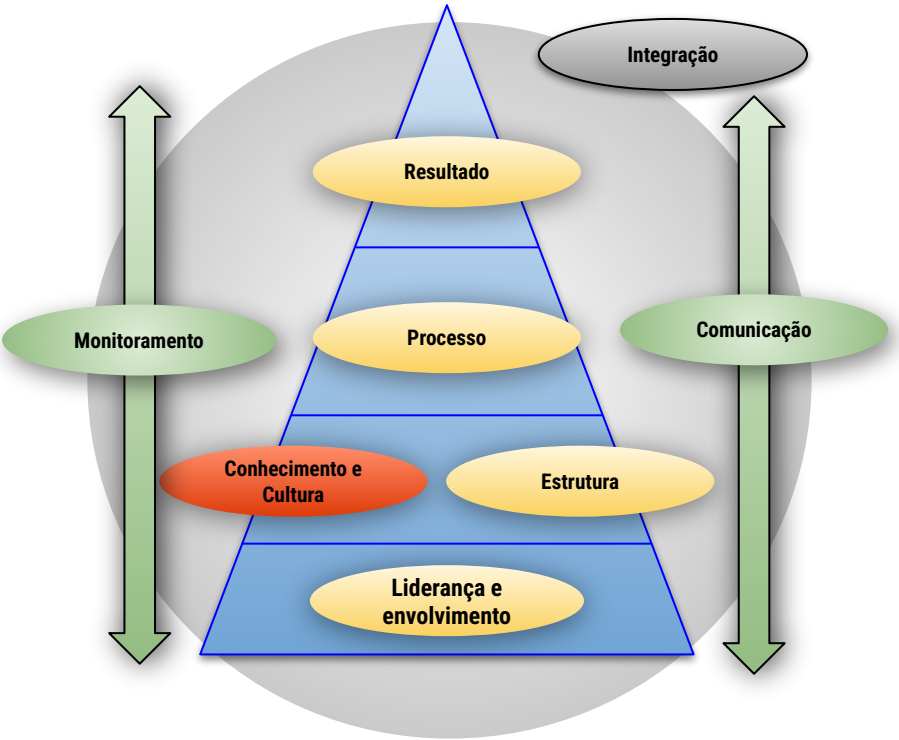


CONCEITO

Conhecimento e cultura organizacional trata das pessoas como parte importante do processo aperfeiçoamento da gestão de riscos e controles internos. Este grupo enfatiza o nível de conhecimento e a consciência dos gestores sobre sua responsabilidade na identificação e gestão de riscos, a a existência de documentos e manuais sobre gestão de riscos e a qualificação dos membros da Unidade de Controle Interno.



2.3 CONHECIMENTO E CULTURA

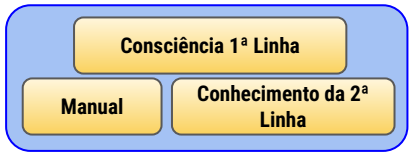


REQUISITOS

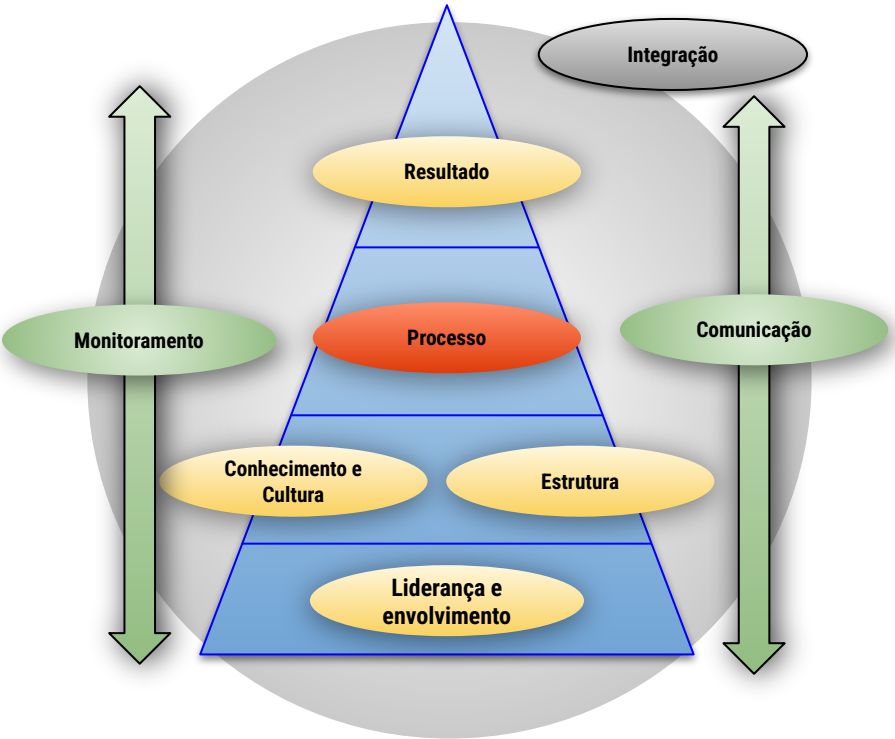
7.Os gestores da **primeira linha** têm consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes.

8. O órgão/entidade dispõe de um **manual de gestão de riscos, ou documento similar**, aprovado pela alta administração, disponível e comunicado às partes interessadas.

9. Os membros da Unidade de Controle Interno (Segunda Linha) possuem **conhecimento suficiente** para conduzir e orientar a gestão de riscos em seu órgão/entidade.



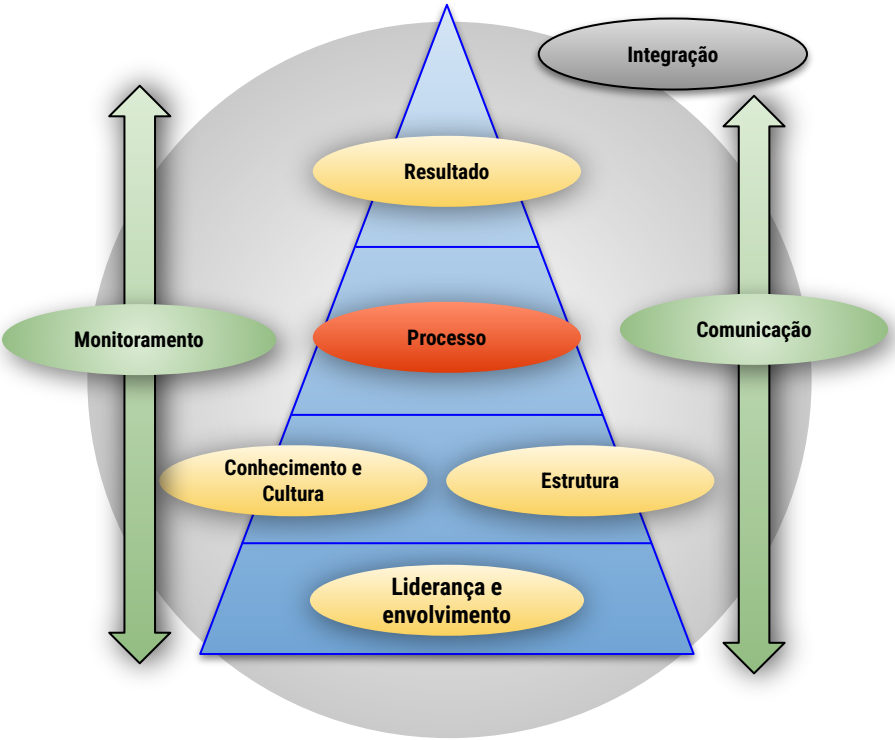
2.5 PROCESSO



CONCEITO

O processo refere-se às **etapas do gerenciamento de riscos**. E para que elas funcione corretamente, é importante a participação dos principais atores da primeira e da segunda linha no processo de gerenciamento de riscos, resultando numa lista de riscos e controles relevantes, evidenciados com os principais documentos que dão suporte às análises e definições.

2.5 PROCESSO



REQUISITOS

10. O gerenciamento dos riscos é realizado por pessoas designadas que têm **responsabilidade**, **autoridade** e **experiência** nas atividades objeto de análise.

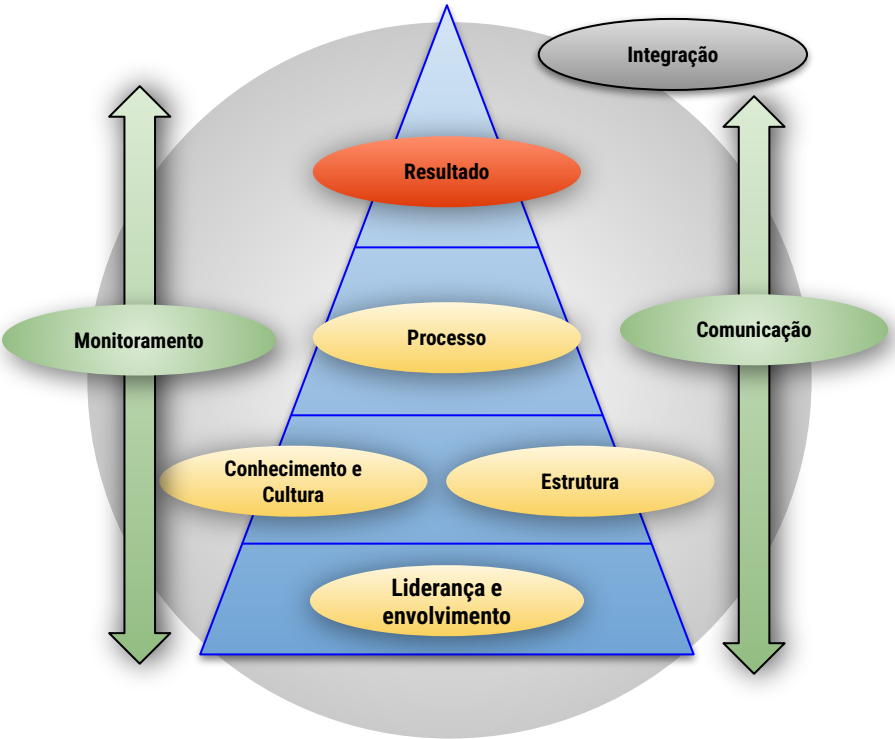
11. A Unidade de Controle Interno (Segunda Linha) apoia o processo de gerenciamento de riscos, fornecendo metodologias e ferramentas às áreas, com a finalidade de identificar e avaliar riscos.

12. O processo de gerenciamento de riscos produz uma lista de **riscos RELEVANTES** e **controles APROPRIADOS**, através da utilização de metodologia consolidada, como às do COSO ou ISO.

13. O órgão/entidade realiza o **registro sistemático das evidências** que suportam a identificação, análise e avaliação dos riscos, a proposição de controles e a avaliação da eficácia desses controles.

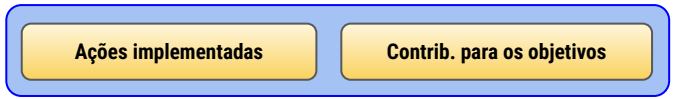
14. O tratamento dos riscos é registrado em **plano de ação e comunicado formalmente** aos responsáveis pela sua implementação, assegurando que compreendam, assumam compromissos e sejam responsáveis por essas ações.

2.6 RESULTADO

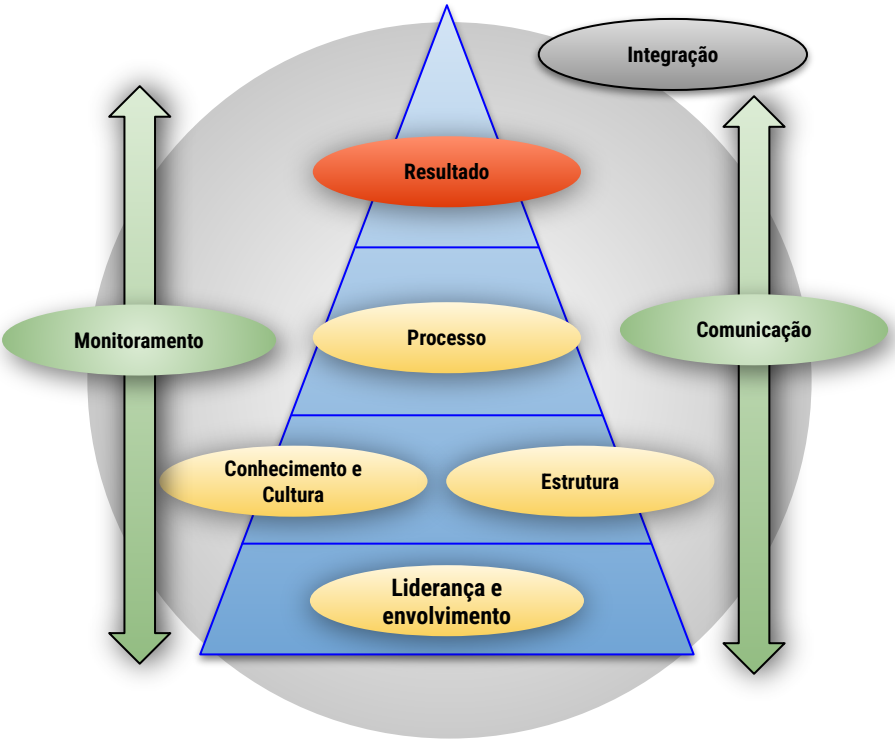


CONCEITO

Este grupo avalia se a **gestão de riscos gera resultados tangíveis**. Num primeiro momento, a avaliação restringe no nível de implementação dos controles propostos. Num segundo, a avaliação foca no impacto no atingimento dos objetivos organizacionais decorrente dos controles implementados.



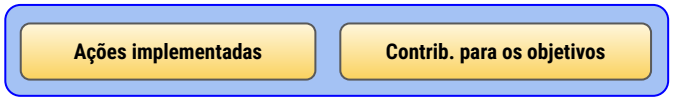
2.6 RESULTADO



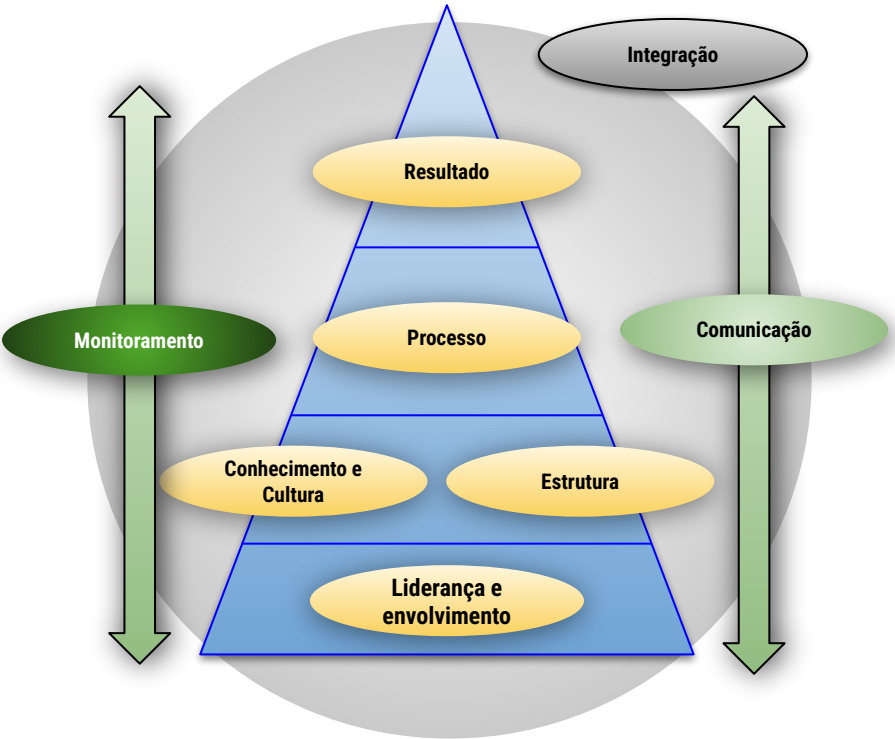
REQUISITOS

15. As **respostas aos riscos** identificados (controles) são implementadas.

16. A gestão de riscos no órgão/entidade está **contribuindo** para o alcance dos seus principais objetivos.

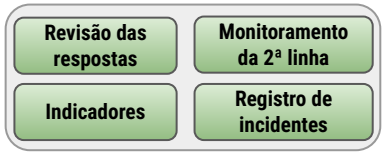


2.7 MONITORAMENTO

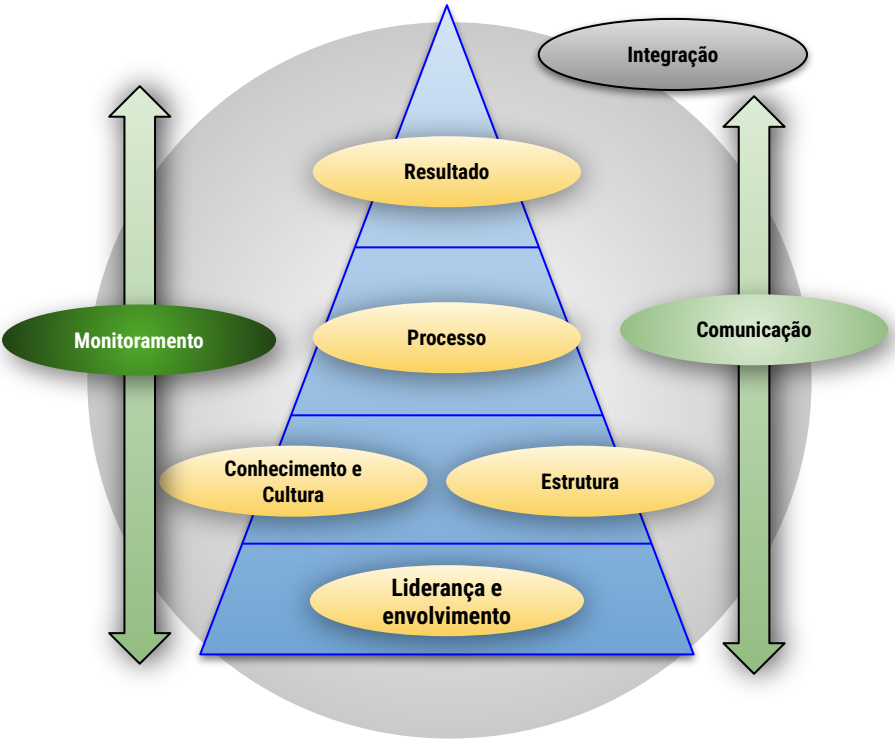


CONCEITO

Este grupo traz as práticas de revisão periódica das respostas ao risco (controles), de estabelecimento de indicadores que permitam **avaliar a efetividade das respostas aos riscos** (controles), da UCI atuando como facilitadora e supervisora no processo de monitoramento dos riscos e da existência da avalia e registro os problemas ocorridos.



2.7 MONITORAMENTO



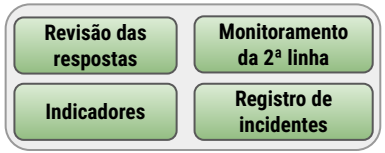
REQUISITOS

17. Existe **monitoramento e revisão periódica dos riscos e das respectivas respostas** (controles), visando avaliar se permanecem adequadas.

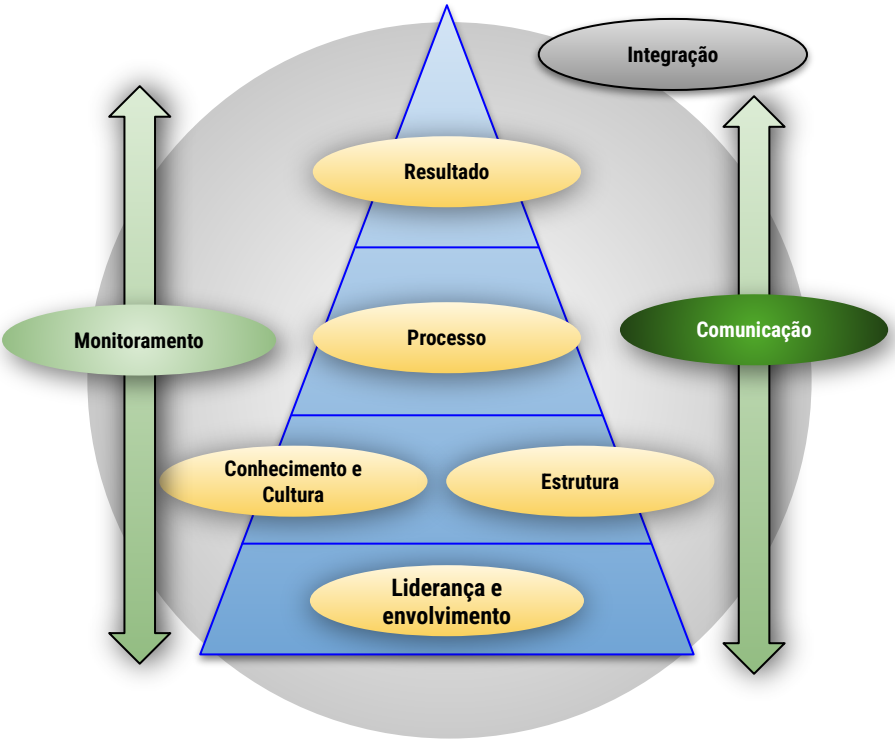
18. São estabelecidos **indicadores** que permitam monitorar os riscos e avaliar a efetividade das respostas aos riscos (controles).

19. A Unidade de Controle Interno (Segunda Linha) atua como **responsável pelo monitoramento da Gestão de Riscos**, verificando se a construção, implementação e resultados do processo de gestão de riscos se concretizam conforme o esperado e comunicando ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos das áreas.

20. A gestão avalia e registra os problemas ocorridos em **documento específico (Ex.: Planilha de Registro de incidentes), realizando a devid**a atualização no gerenciamento de riscos, quando necessário.

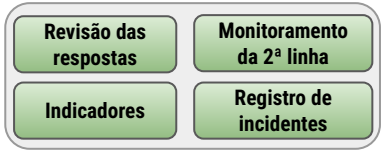


2.8. COMUNICAÇÃO

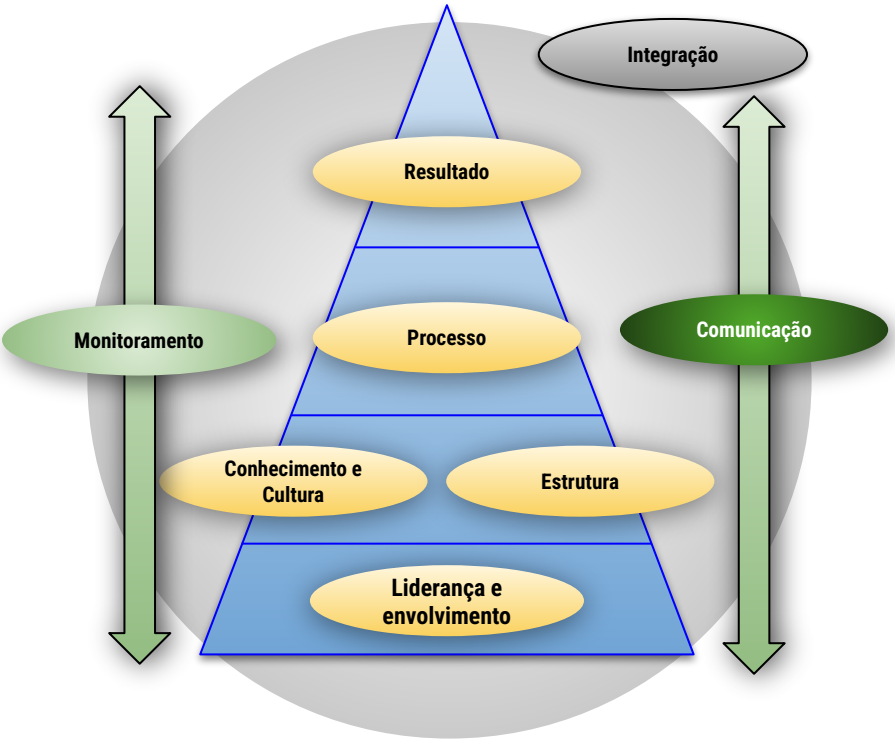


CONCEITO

A comunicação busca promover a conscientização e o entendimento do risco, bem como a existência de mecanismos para informar tempestivamente sobre o processo e a eficácia da gestão de riscos.



2.8. COMUNICAÇÃO



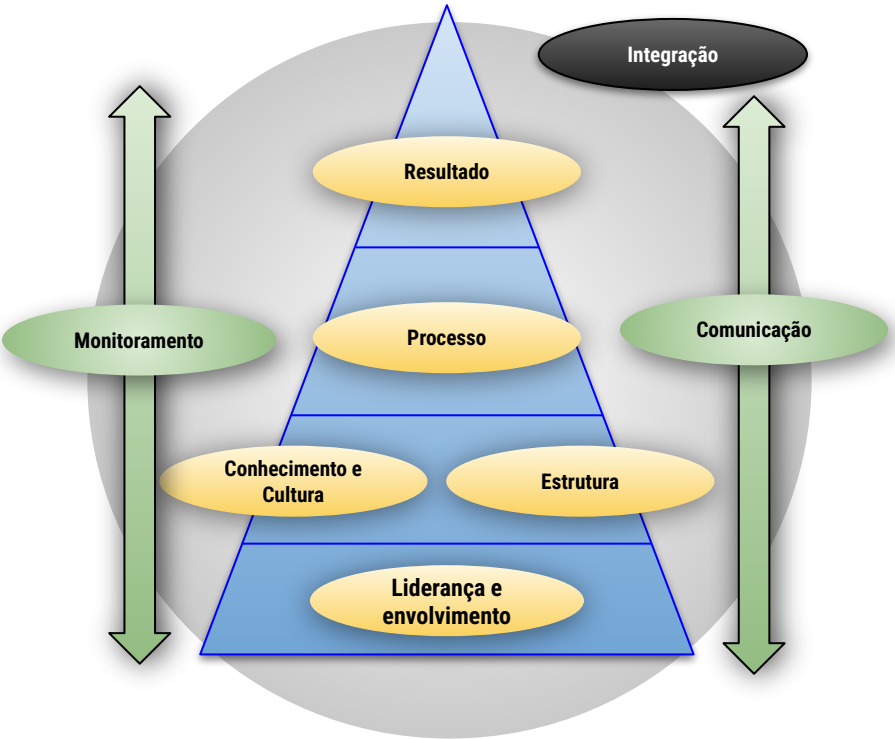
REQUISITOS

21. O órgão/entidade realiza campanhas, palestras e/ou outros atos de sensibilização sobre a importância de gerenciar riscos.

22. Existem **mecanismos de comunicação** formalizados através de plano de comunicação e em execução que garantam que as partes interessadas recebam informações **tempestivas, claras e relevantes** sobre o processo de gestão de riscos e a sua eficácia no órgão/entidade.

Revisão das respostas	Monitoramento da 2ª linha
Indicadores	Registro de incidentes

2.9 INTEGRAÇÃO



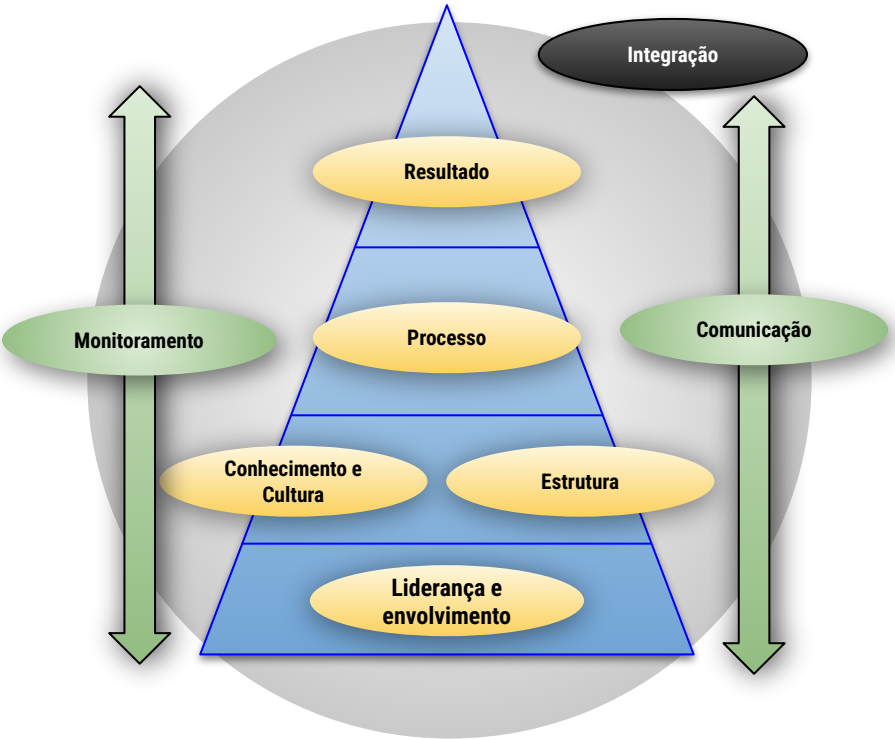
CONCEITO

Reforça a importância de integrar a gestão de riscos em todos os processos organizacionais, desde a tomada de decisão até a execução. Este grupo trata da **integração entre a gestão de riscos e o planejamento** e da **abrangência de setores da organização que conhecem os seus riscos críticos.**

Monitoramento integrado

Riscos de áreas, funções e atividades relevantes

2.9 INTEGRAÇÃO



REQUISITOS

23. O monitoramento dos riscos e controles é realizado de forma integrada com o monitoramento dos objetivos estratégicos, metas e indicadores da organização.

24. As principais áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) têm identificados os **riscos críticos** de sua atuação para a realização dos principais objetivos da organização.

Monitoramento integrado | Riscos de áreas, funções e atividades relevantes

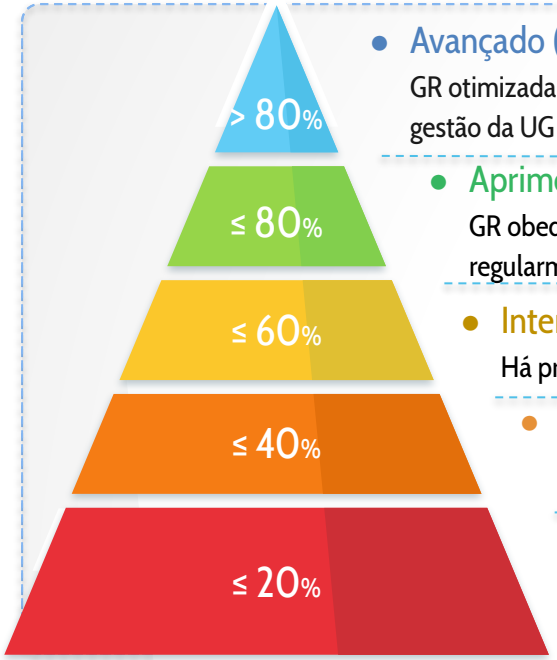
03 NÍVEIS DE MATURIDADE

3.1 PESOS DOS GRUPOS DE PRÁTICAS

Nº	Agrupamento	Peso
1	Liderança e Envolvimento	6,00%
2	Estrutura	3,70%
3	Conhecimento e Cultura	26,80%
4	Processo	12,70%
5	Resultado	31,50%
6	Monitoramento	8,50%
7	Comunicação	5,10%
8	Integração	5,70%
Total		100,00%

Obs.: Pesos definidos com base no método estatístico AHP – Analytic Hierarchy Process.

3.2 NÍVEIS DE MATURIDADE



- **Avançado ("Habilitado")**
  GR otimizada; Princípios e processos de GR integrados aos processos de gestão da UG
- **Aprimorado ("Gerenciado")**
  GR obedece aos princípios estabelecidos; é supervisionada e regularmente aprimorada
- **Intermediário ("Definido")**
  Há princípios e padrões documentados, e treinamento básico sobre GR
- **Básico ("Consciente")**
  GR tratada informalmente; Ainda não há treinamento e comunicação sobre riscos
- **Inicial ("Ingênuo")**
  Baixo nível de formalização; Documentação sobre GR não disponível; Ausência de comunicação sobre riscos

OBRIGADO!

PARA MAIS DÚVIDAS

gestaoderiscos@scge.pe.gov.br
3183-0906
https://www.scge.pe.gov.br/gestao-de-riscos/

CF

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

Gestão de Riscos
SCGE-PE