Enap Escola Nacional de Administração Pública

Gestão de Riscos no Banco Central do Brasil

Isabela Ribeiro Damaso Maia
Departamento de Riscos Corporativos e Referências Operacionais
Agosto/2017

BANCO CENTRAL DO BRASIL

Enap MINISTÉRIO DO PLANEJAMENTO

BRASIL GOVERNO FEDERAL

Agenda

1. *Introdução*
2. *Dualidade do Risco*
3. *Governança*
4. *Dimensões de Risco*
5. *Desafios*
6. *Considerações Finais*

1. Introdução

Definições

- *O que é* **Incerteza***?*

  Impossibilidade de se assegurar qualquer evento futuro.

- *O que é* **Risco***?*

  Incerteza mensurada por meio de uma distribuição de probabilidade.

- *O que é* **Impacto***?*

  Consequência do evento.

- *O que é* **Causa***?*

  Fatores que podem contribuir para a ocorrência de um evento.

E o COSO?

COSO's structure and mission

- COSO is a joint initiative of five sponsoring organisations
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Financial Executives International (FEI)
  - Institute of Management Accountants (IMA)
  - Institute of Internal Auditors (IIA)

COSO's mission is…

"…to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."

www.coso.org/aboutus.htm

Risco – ISO 31000

O que é ?

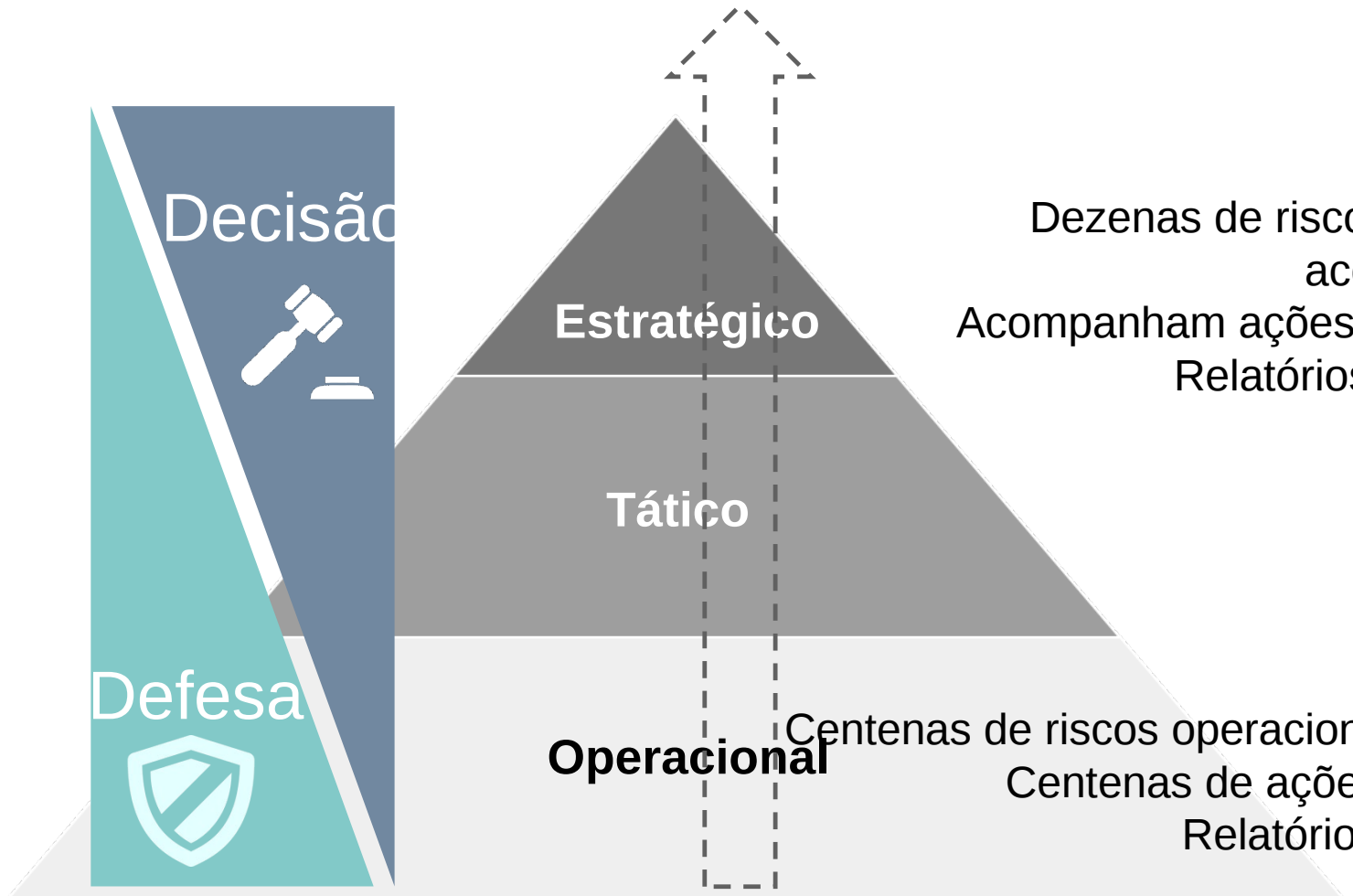
- *A gestão de riscos é parte da tomada de decisões;*
- *A gestão de riscos cria e protege valor;*
- *A gestão de riscos é parte integrante de todos os processos organizacionais;*
- *A gestão de riscos é sistemática, estruturada e oportuna;*
- *A gestão de riscos é feita sob medida*
- *A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.*

O que não é ?

- **Não tem foco em controle.**
- **Não envolve conformidade.**
- **Busca o futuro e não checar o passado**.

2. Dualidade do Risco

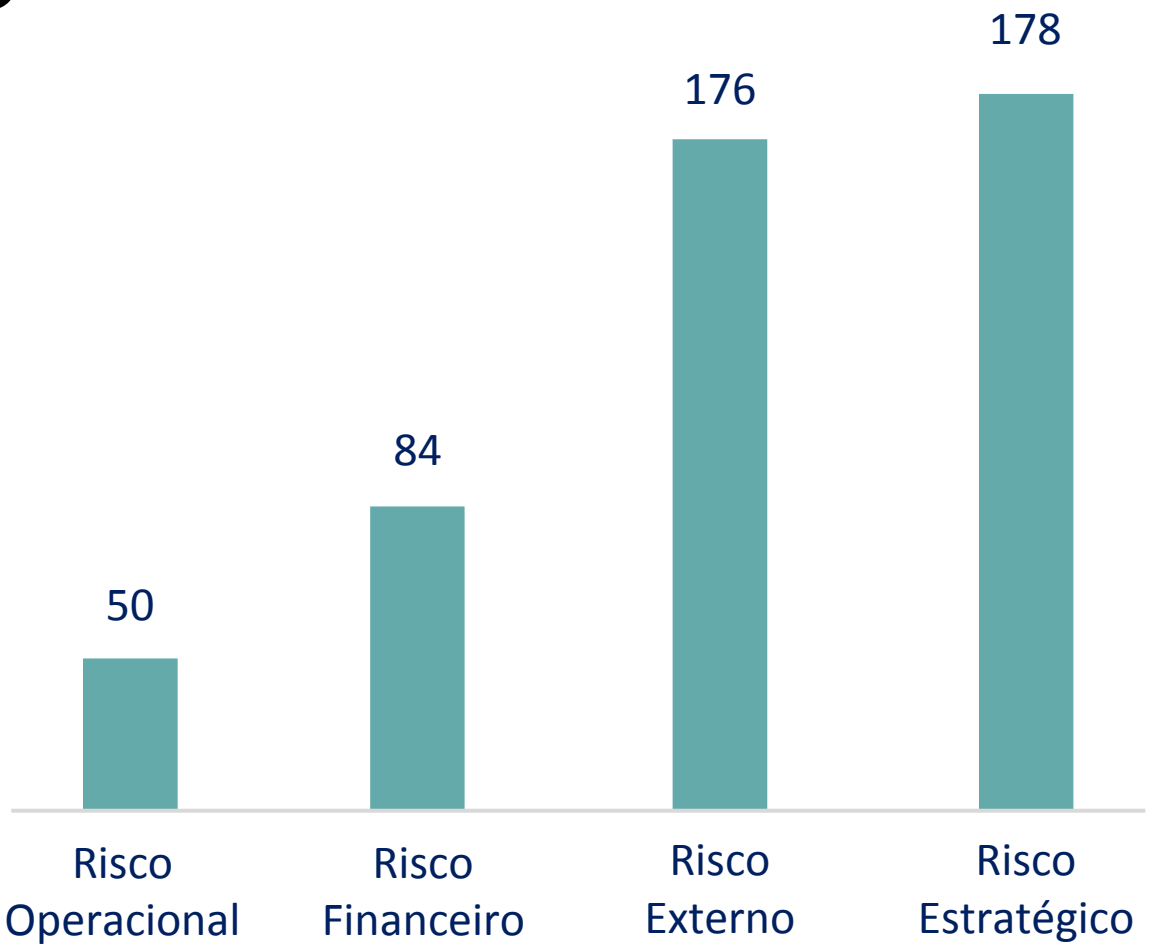
Dualidade do Risco



Dezenas de riscos relevantes acompanhados
Acompanham ações estratégicas
Relatórios + sintéticos

Centenas de riscos operacionais levantados
Centenas de ações de mitigação
Relatórios + detalhados

Motivação



Fonte: The value killers revisited – A risk management study

Deloitte.

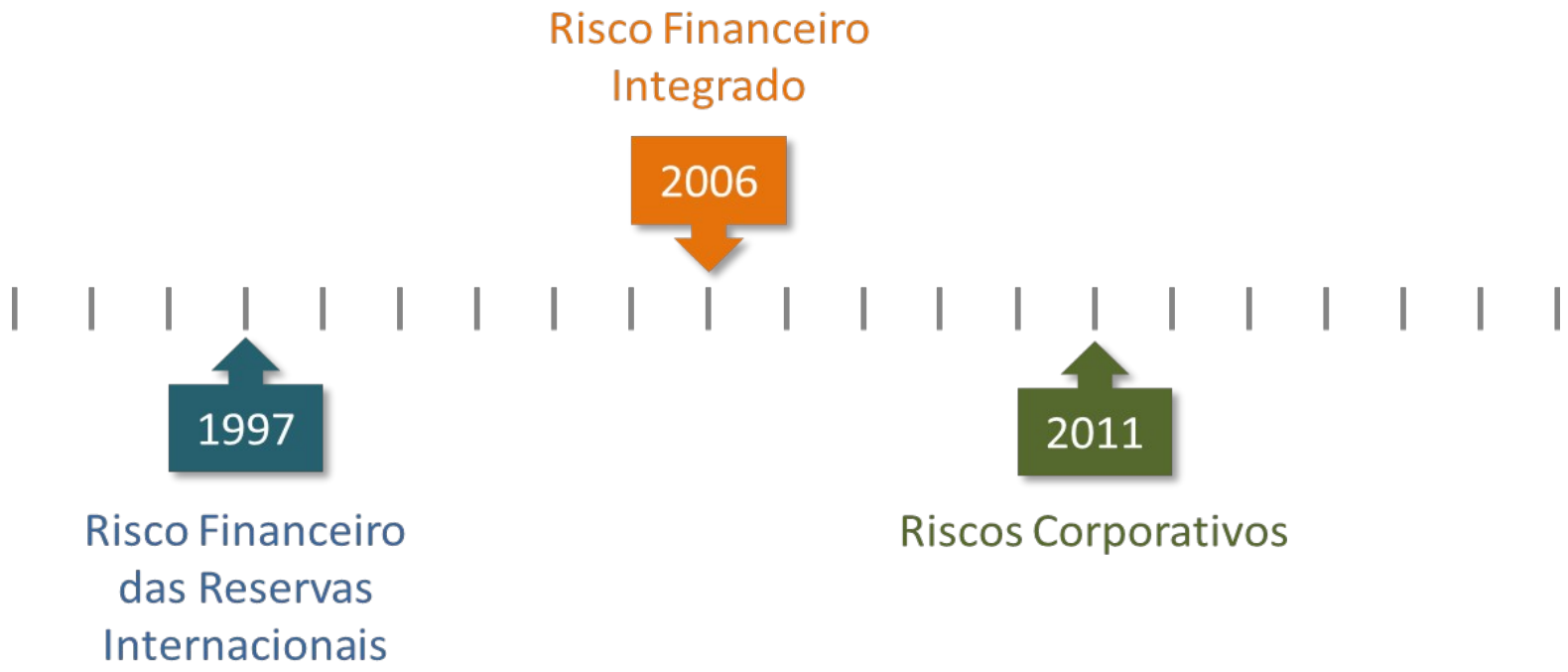
Enap Escola Nacional de Administração Pública

ERM: Visão Holística

De uma cultura baseada em silos para uma gestão integrada dos riscos

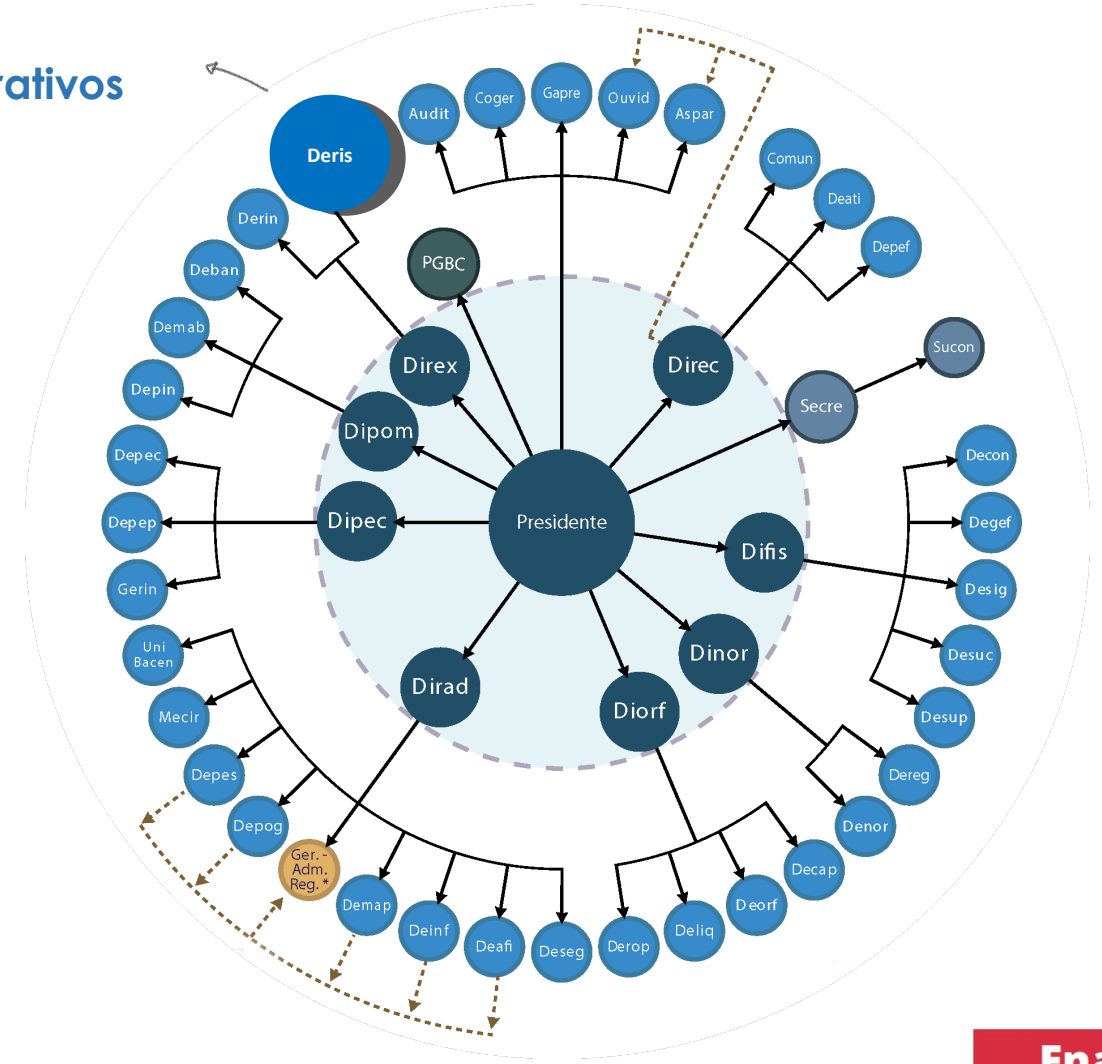
3. Governança

Linha do Tempo



Estrutura Organizacional

Departamento de Riscos Corporativos e Referências Operacionais



Estrutura de Risco

Comitê de Governança, Riscos e Controle Interno (Diretoria Colegiada)

Diretor de Assuntos Internacionais e de Gestão dos Riscos Corporativos

Departamento de Riscos Corporativos e Referências Operacionais

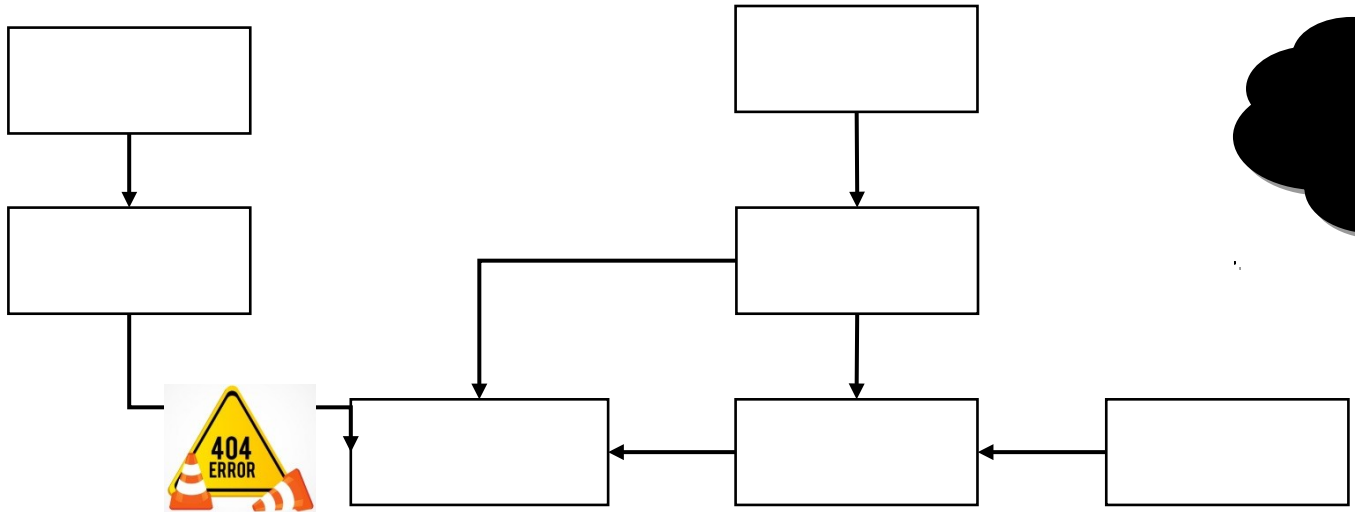
AGR

Riscos financeiros e referências operacionais	Riscos não financeiros	Continuidade de negócios

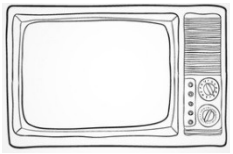
• Alocação estratégica de ativos
• Risco de Mercado
• Risco de Crédito
• Risco de Liquidez
• Mensuração de resultados
	• Risco Operacional
	  • Negócios
	  • Reputacional
	  • Financeiro
	• Risco Estratégico
		• BIA
		• ARC
		• Simulações e Testes
		• Cartão de Continuidade
		• TEIC
		• Plano de Continuidade

4. Dimensões de Risco

Risco Operacional



Impactos:



reputacional

financeiro

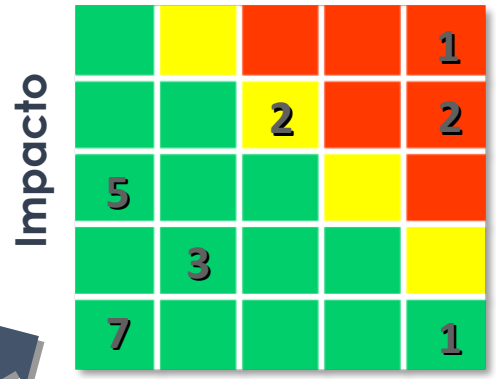
negócio

Riscos Operacionais

Identificação e mensuração

- RCSA
- Indicadores Chave de Risco
- Registro Histórico de Eventos

Avaliação (Matriz de Riscos)



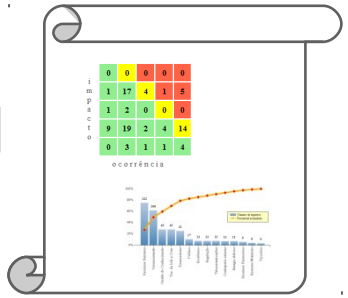
Tratamento

prioridade para tratamento

III *menor* II *média* I *maior*

Classes de Risco

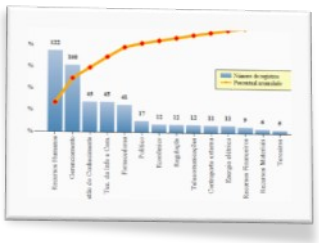
Mitigar
Aceitar
Transferir
Eliminar



Comunicação aos Diretores

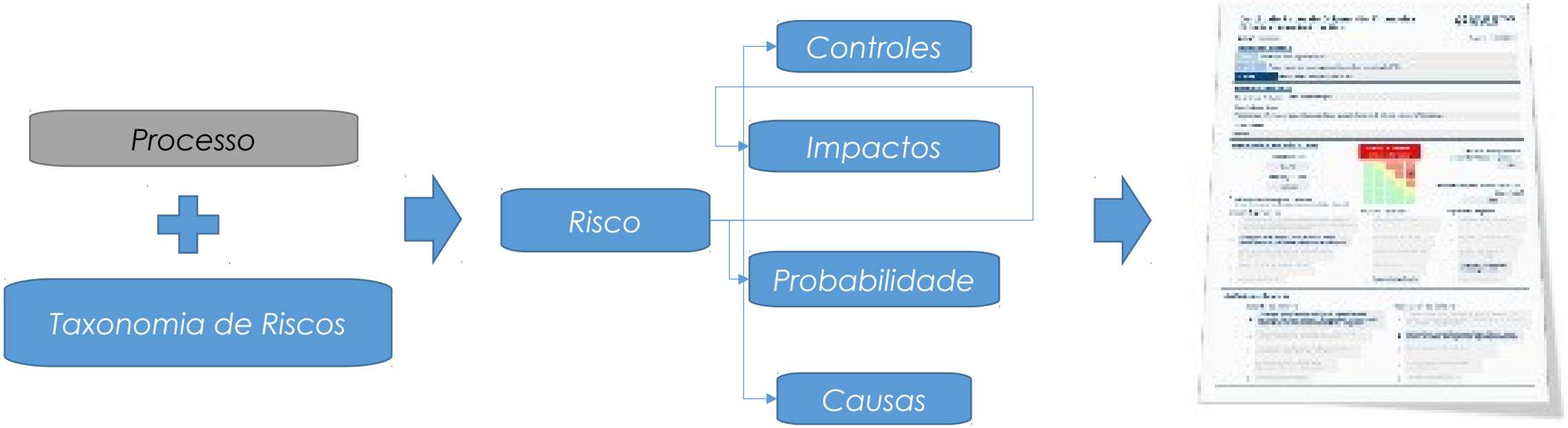
Comunicação e Ação com Áreas Suporte

Planos de Mitigação de Riscos (PMRs)



Informações agregadas (TI, planejamento, RH, treinamento)

RCSA

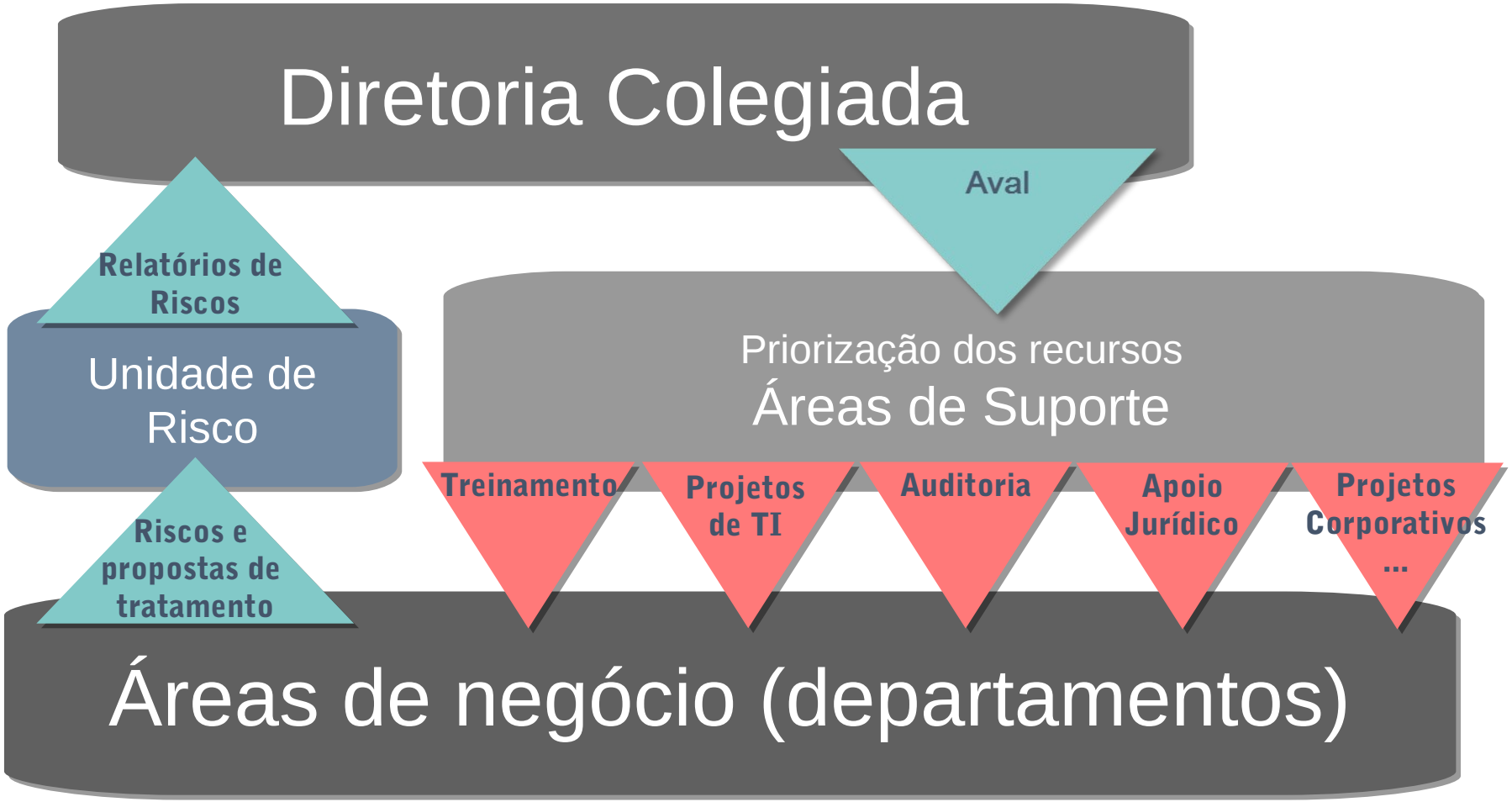

Processo
Taxonomia de Riscos
Risco
Controles
Impactos
Probabilidade
Causas

Registro Histórico de Eventos - RHE

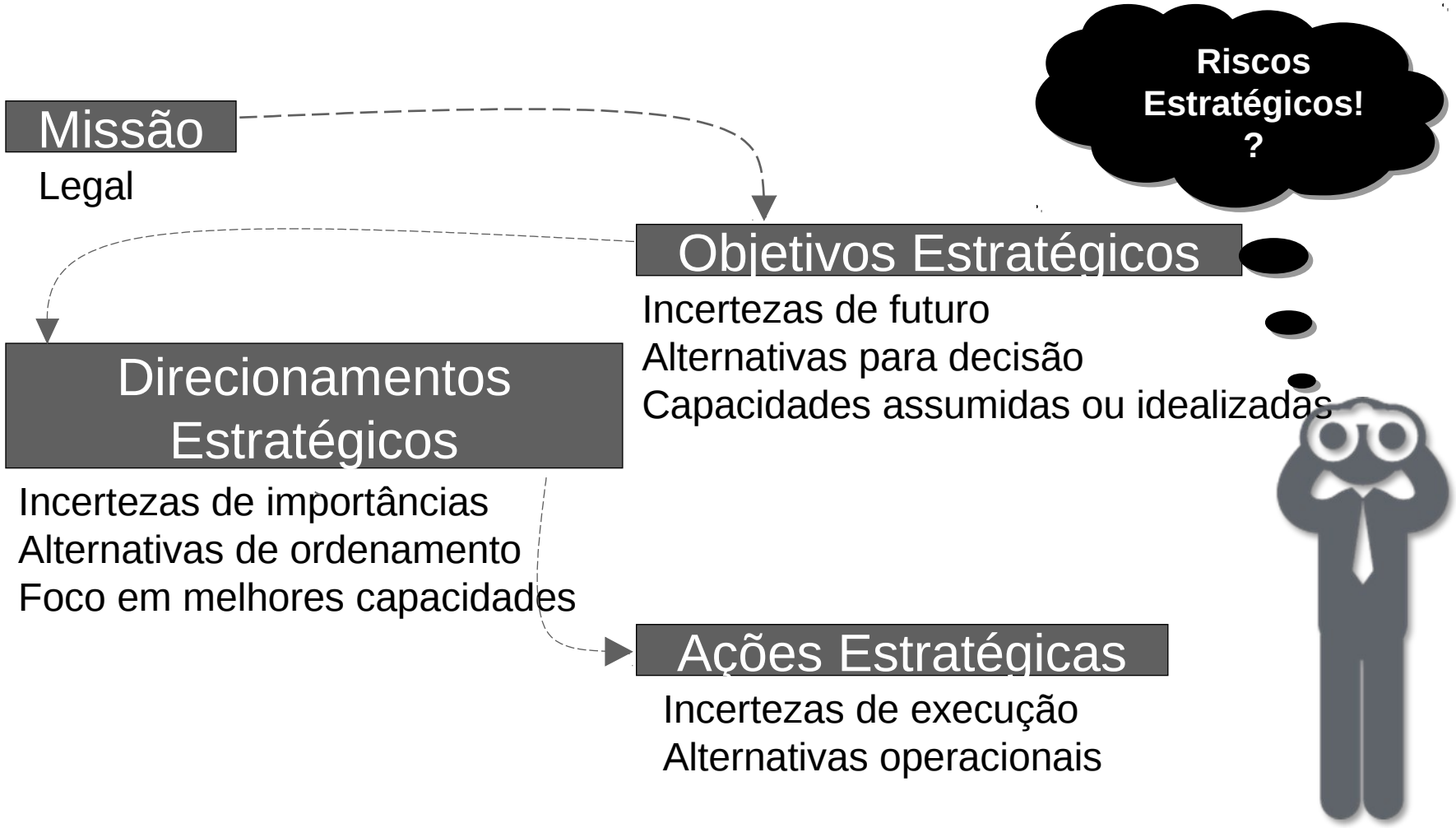
- *Reduzir a subjetividade*
  - *formar base de dados a partir de dados internos e/ou externos (consórcios ou de instituições similares)*
  - *Permite análise histórica dos eventos (tendência, revisão do RCSA)*
- *Todos os eventos ou quase eventos devem ser registrados, independente da severidade do impacto*
- *Monitoramento*

Indicadores Chave de Risco - ICR

Apoio à decisão



Risco Estratégico



Risco Estratégico

Diagnóstico

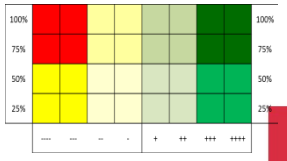
Análise Retrospectiva
Análise de Riscos

Formulação Estratégica

Missão, Visão, Valores e Objetivos Estratégicos

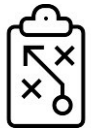
Riscos Estratégicos

Avaliação de Riscos Estratégicos



Desdobramento da Estratégia

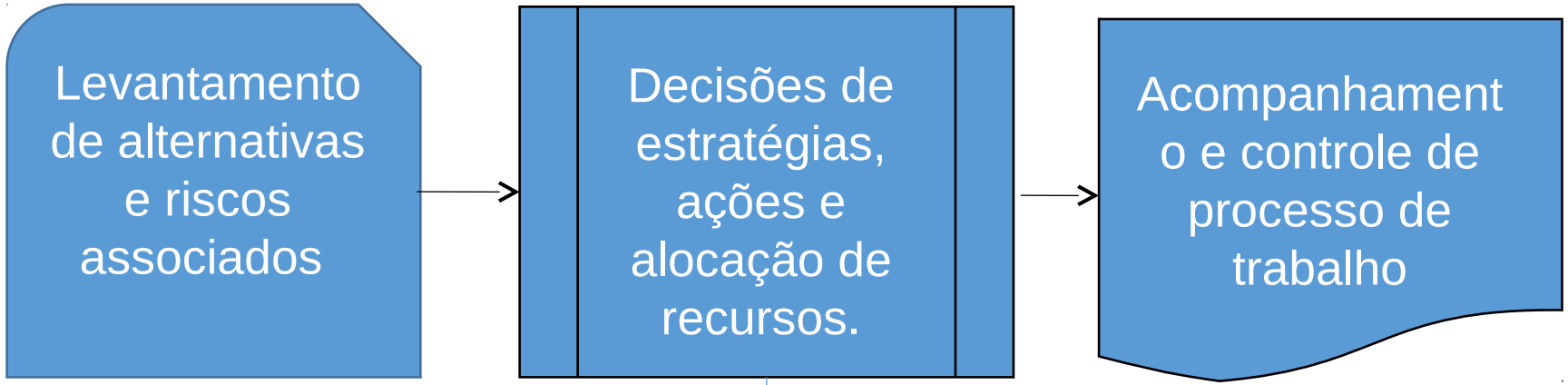
Execução das Ações



Implantação

Monitoramento

Apoio à decisão



Antes do processo decisório:
- Riscos transversais
- Análise de causas recorrentes
- Oportunidades

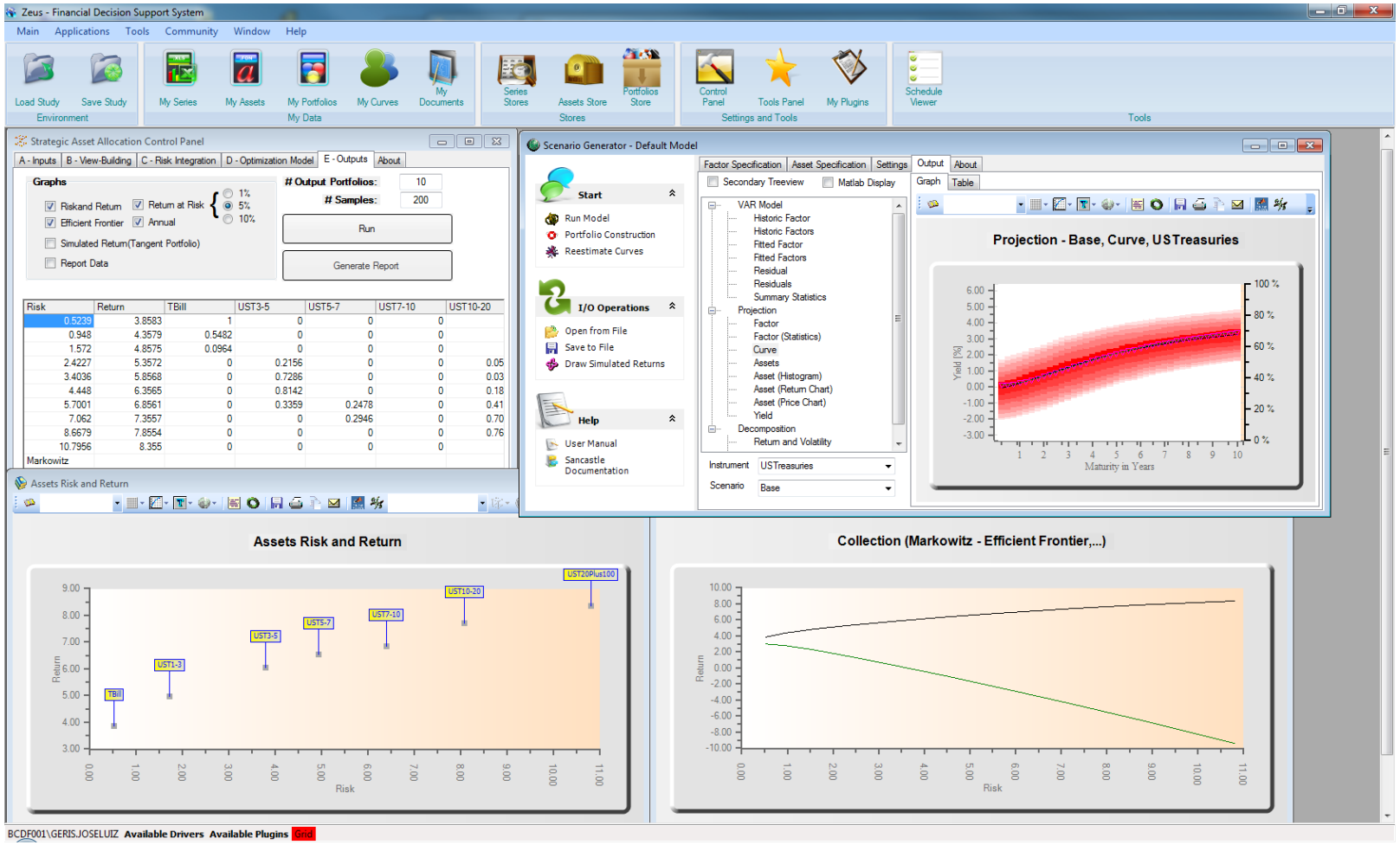
\+ Riscos externos

...

Depois do processo decisório:
- Avaliação dos controles
- Continuidade de negócios
- Riscos operacionais
- ...

Fonte dos principais problemas corporativos!

Riscos Financeiros



Continuidade de Negócios

Processos na Cadeia de Valor

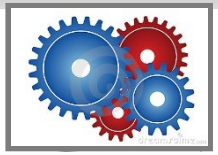
P1 P2 P3 P4 P5
P6 P7 P8 P9 ...
PN

Classificação pela urgência

P1 P6	P3	P9	P15
DO	D1	D5	D21

BIA COMPLETA

BIA SIMPLIFICADA



PCN NÍVEL 3 e 4

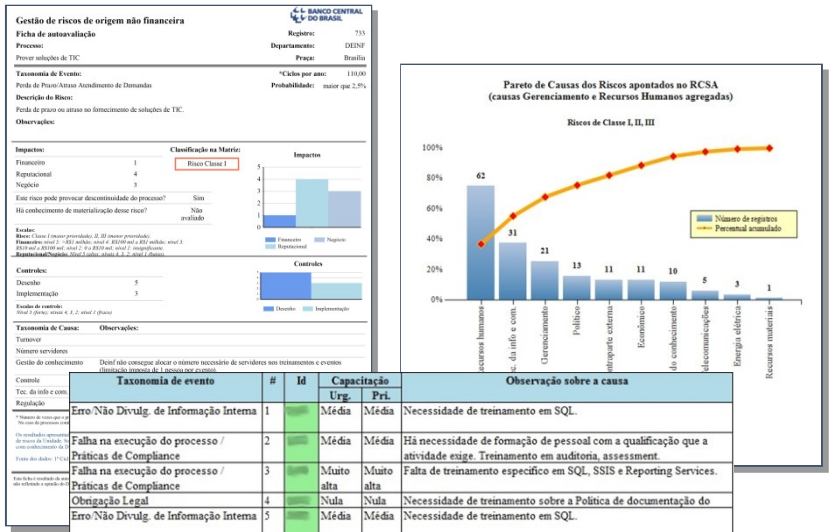
PCN NÍVEL 2

PCN NÍVEL 1

Cartão de Continuidade

Ferramentas de Suporte à Gestão de Risco

Ficha de Risco
Relatórios Dinâmicos


Gestão de riscos de origem não financeira

Ficha de autoavaliação

Processo:

Prover soluções de TIC

Registro: 733

Departamento: DEINF

Praça: Brasília

Taxonomia de Evento:

Perda de Prazo/Atraso Atendimento de Demandas

Descrição do Risco:

Perda de prazo ou atraso no fornecimento de soluções de TIC.

Observações:

*Ciclos por ano: 110,00

Probabilidade: maior que 2,5%

Impactos:

Financeiro	1
Reputacional	4
Negócio	3

Classificação na Matriz: Risco Classe I

Este risco pode provocar descontinuidade do processo? Sim

Há conhecimento de materialização desse risco? Não avaliado

Controles:

Desenho	5
Implementação	3

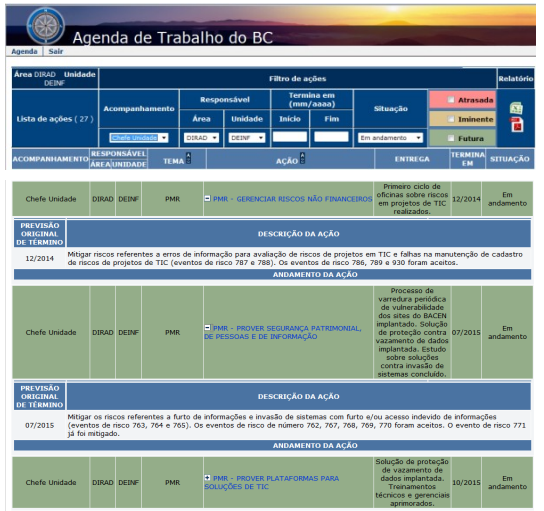
Taxonomia de Causa: Observações:

Turnover	
Número servidores	
Gestão do conhecimento	Deinf não consegue alocar o número necessário de servidores nos treinamentos e eventos (limitação imposta de 1 nesses por evento).
Controle	
Tec. da info e com.	
Regulação	

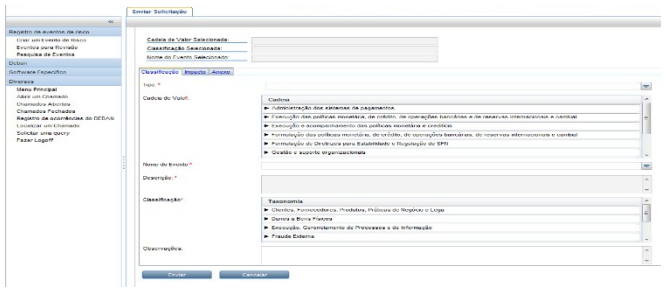
Taxonomia de evento	#	Id	Capacitação		Observação sobre a causa
			Urg.	Pri.	
Erro/Não Divulg. de Informação Interna	1		Média	Média	Necessidade de treinamento em SQL.
Falha na execução do processo / Práticas de Compliance	2		Média	Média	Há necessidade de formação de pessoal com a qualificação que a atividade exige. Treinamento em auditoria, assessment.
Falha na execução do processo / Práticas de Compliance	3		Muito alta	Muito alta	Falta de treinamento especifico em SQL, SSIS e Reporting Services.
Obrigação Legal	4		Nula	Nula	Necessidade de treinamento sobre a Politica de documentação do
Erro/Não Divulg. de Informação Interna	5		Média	Média	Necessidade de treinamento em SQL.
Falha na execução do processo / Práticas de Compliance	6		Média	Média	Necessidade de treinamentos internos para compartilhar conhecimentos especificos e extensos.
Falha na execução do processo / Práticas de Compliance	7		Média	Média	Necessidade de treinamentos internos para compartilhar conhecimentos especificos e extensos. Necessidade de vivência na
Erro de Informação	8		Muito alta	Muito alta	Falta de treinamento em, por exemplo, SQL e SAS.
Falha na execução do processo / Práticas de Compliance	9		Alta	Alta	Falta de treinamento nas áreas de Finanças e Economia (principalmente Politica Monetária).
Falha na execução do processo / Práticas de Compliance	10		Muito alta	Muito alta	Falta de treinamento especifico em SQL, SSIS e Reporting Services.

Monitoramento de Riscos

Registro dos PMRs



Registro Histórico de Eventos

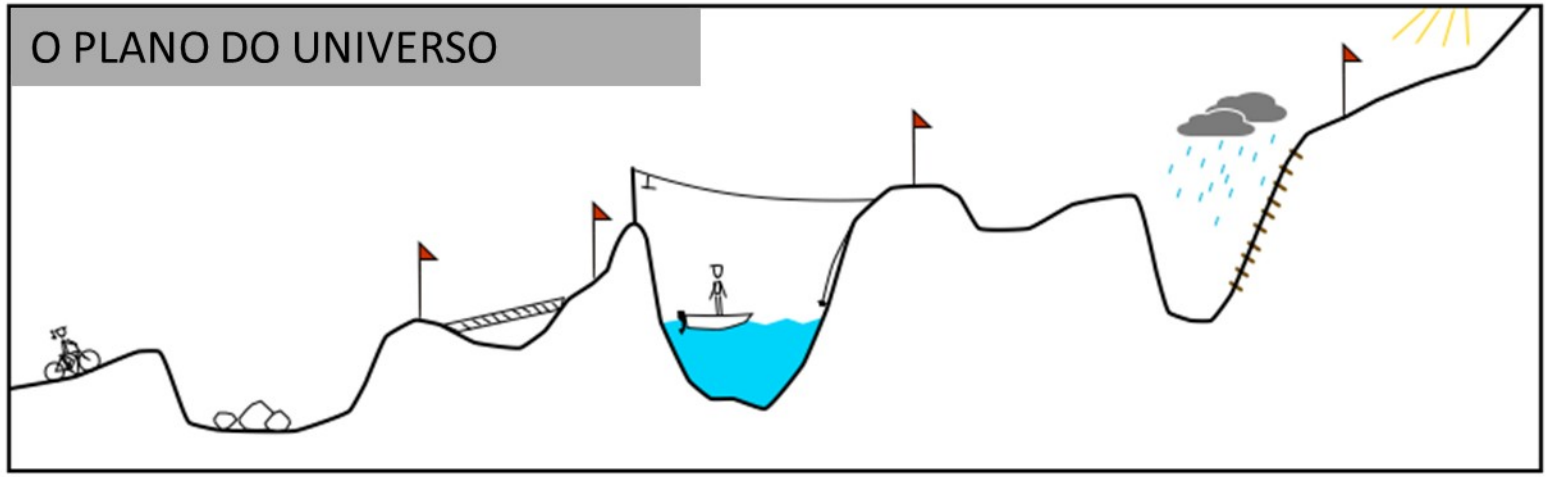


5. Desafios

Desafios

Curva de Mudança

Como implantar a gestão de riscos?



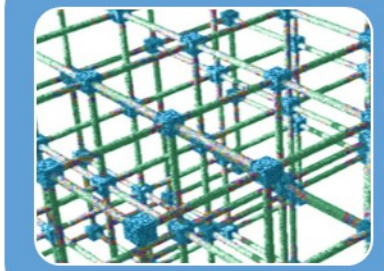
Desafios

- ✓ *Identificação de riscos baseada na Cadeia de Valor*
- ✓ *Construção da cultura de riscos*
- ✓ *Capacitação dos Agentes de Gestão de Risco*
- ✓ *Levantamento de informações detalhadas*
- ✓ *Workshop de Risk and Control Self Assessment*
- ✓ *Construção de base de dados uniforme*
- ✓ *Construção de Indicadores Chave de Risco*
- ✓ *Registro dos incidentes*
- ✓ *Ferramentas (armazenamento e monitoramento das informações)*
- ✓ *Comunicação*

Apoio à decisão

5. Considerações Finais

ERM - O que se espera da Área de Risco



- Promover a cultura de risco;
- Riscos mapeados de forma sistemática e uniforme em toda a instituição;
- Comunicar os riscos com objetividade;
- Estabelecer de forma clara a propriedade dos riscos;

- Instituição comprometida com os planos de mitigação;
- Riscos alinhados à tolerância da organização;
- Indicadores de risco capazes de antecipar potenciais eventos.

- Apoiar o processo decisório:
- Favorecer o alcance dos objetivos estratégicos;

Gestão de Risco

Etapas para implantação

- ✓ *Aprovar Governança da Gestão dos Riscos*
- ✓ *Estabelecer a Política de Gestão de Riscos*
- ✓ *Mapeamento da Cadeia Valor*

- ✓ *Definir metodologia e ferramenta para mapeamento e monitoramento dos riscos operacionais*
  - ✓ *Dimensões, métricas, propriedade...*
  - ✓ *Abordagem para tratamento de riscos*
  - ✓ *Apoio à decisão (comunicação dos riscos)*
- ✓ *Definir critérios de Registros de Eventos*

- ✓ *Incluir outras dimensões de risco (estratégico, legal, projetos, financeiros, idiossincráticos...)*
- ✓ *Incluir dimensão de Gestão de Continuidade de Negócio*
- ✓ *Definir critérios de ICR*
- ✓ *Ampliar processo de apoio à tomada de decisão com informações de risco*

FIM