GESTÃO DE RISCOS

PAULA SOARES DE ALMEIDA

UNIFEI - UNIVERSIDADE FEDERAL DE ITAJUBÁ

AGOSTO, 2016.

CONTEXTO

- Auditoria Interna - Atividade independente e de assessoria à gestão;

- Auxilia a organização a atingir seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e **melhorar a eficácia dos processos de gerenciamento de riscos**, dos controles internos, da integridade e da governança. (Instituto dos Auditores Internos do Brasil- IIA Brasil e CGU IN Conjunta nº1, maio 2016)

CAMADAS DE DEFESA DA GESTÃO (CGU IN 01-05/2016)

ACÓRDÃOS TCU DE 2013 E 2014

- TCU Acórdãos Plenário nº 3392/2013, 3388/2013, 3383/2013, 3466/2014...
- TCU Acórdão nº 3821/2014 – Plenário: importância do gerenciamento de riscos nas organizações ao afirmar ser de sua competência a intensificação de ações que promovam a melhoria da gestão de riscos e dos controles da Administração Pública;

9.17.3. estruture mais adequadamente as práticas de planejamento estratégico adotadas pela organização, com vistas a implementação futura de uma gestão orientada à governança e à gestão de riscos;

9.17.4. promova estudos com vistas a estruturar um sistema de controle interno que enseje a identificação dos riscos mais significativos para os objetivos da organização e o desenvolvimento de controles internos voltados à mitigação ou eliminação desses riscos;

INSTRUÇÃO NORMATIVA CONJUNTA Nº 1, 10 DE MAIO DE 2016 (MINISTÉRIO DO PLANEJAMENTO E A CGU)

- Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;
- Conceitos importantes;
- Cap.II Controles Internos da Gestão

Seção III - Estrutura dos Controles Internos da gestão(COSO): ambiente de controle, avaliação de risco, atividades de controle internos, informação e comunicação, monitoramento.

CAP. III DA GESTÃO DE RISCOS
SEÇÃO III – DA ESTRUTURA DO MODELO DE GESTÃO DE RISCOS

I- Ambiente Interno (Base, valores éticos, competências)

II- Fixação dos objetivos (todos os níveis da organização)

III- Identificação de eventos (identificar os riscos às atividades da organização em todos os níveis)

IV- Avaliação dos riscos (probabilidade e impacto- gestores)

V- Resposta ao risco (evitar, transferir, aceitar ou tratar o risco)

VI- Atividades de Controle interno (políticas e procedimentos definidos para mitigar o risco que a organização optou por tratar)

VII- Informação e Comunicação (As informações produzidas devem fluir por todos os níveis de forma clara e aberta à todos)

VIII- Monitoramento (avaliar a qualidade da gestão de riscos e realizar as alterações quando houver alguma alteração na exposição ao risco)

CAPÍTULO III
SEÇÃO VI- POLÍTICA DE GESTÃO DE RISCO

- Prazo para implantação: 11/05/2017

- Art. 18. Considerar os possíveis tipos de risco:
- **Risco operacional**: eventos que podem comprometer as atividades da Universidade, estão associados à falhas de processos internos, pessoas, infraestrutura e sistemas;

Exemplo: Pagamento indevido à servidor que solicitou auxílio transporte mas não anexou o comprovante de endereço no sistema (falha operacional, falha de sistema, falha de controle)

Alunos não terem acesso à notas (Falha no sistema acadêmico)

- **Risco imagem/reputação:** eventos que podem comprometer a confiança da sociedade em relação à missão institucional da Universidade;

Exemplo: Ocorrência de fraudes de conhecimento da sociedade sem a devida punição;

- **Riscos Legais:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da universidade;

Exemplo: Risco de não observância em alteração de normativo. Número de professores afastados acima do permitido para o período, prejudicando os discentes.

- **Riscos Financeiros/orçamentários:** eventos que podem comprometer a capacidade da universidade de contar com recursos financeiros para a realização de suas atividades ou comprometer a própria execução orçamentária.

Exemplo: Risco financeiro: Atraso no envio de recursos financeiros.

Risco orçamentário: Limite de empenho imposto pelo MEC.

CAPÍTULO V – COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES

- Composição do Comitê: Dirigente máximo (Reitor) + Dirigentes subordinados ao Reitor + apoiado pelo Assessor Especial de Controle Interno.
- Competências.

Sua Instituição já tem tudo isto formalizado?

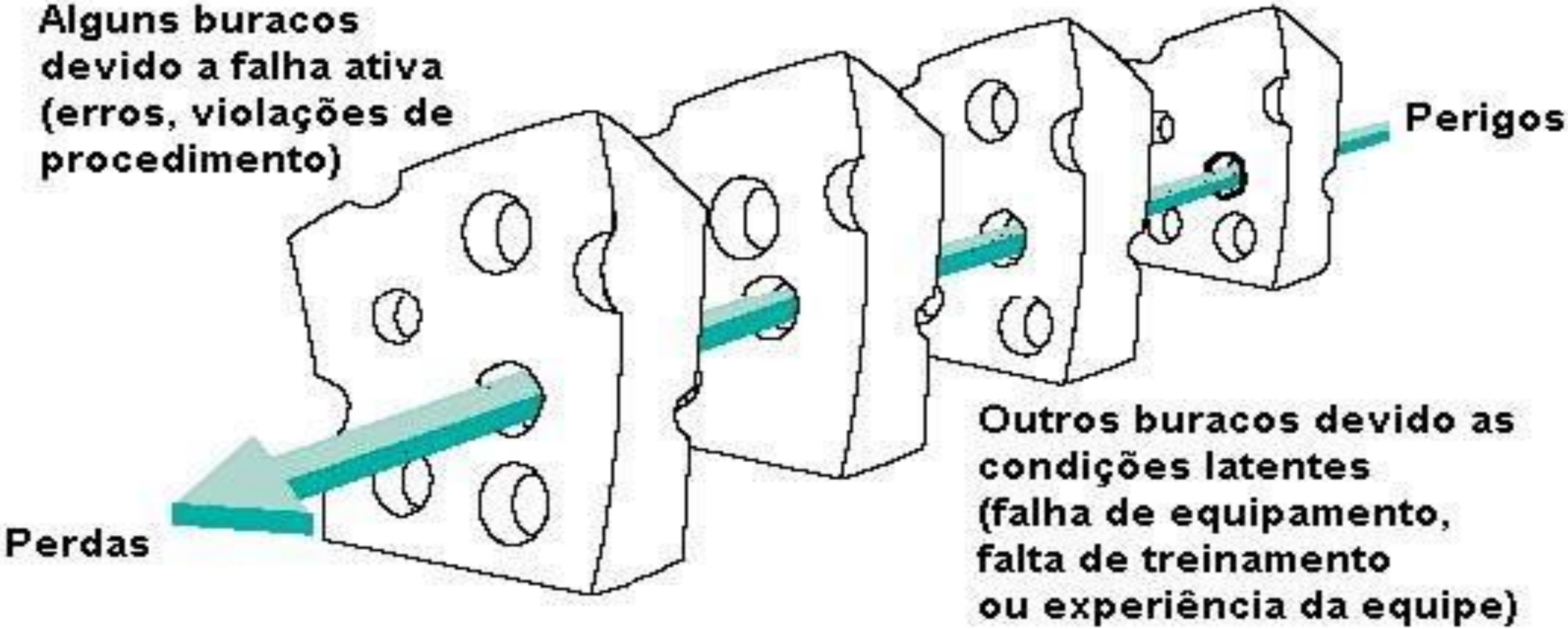
NORMAS SOBRE GESTÃO DE RISCOS

- ABNT NBR ISO 31000:2009 -Gestão de Riscos – Princípios e Diretrizes
- ABNT NBR ISO/IEC 31010:2012 - Gestão de Riscos - Técnicas para o processo de avaliação de riscos.
- *Enterprise Risk Management* (*ERM*)
- *Management of Risk –Principles and Concepts* (*Orange Book)*

ABNT NBR ISO 3100:2009

- Conceitos em geral (Risco = O efeito da incerteza nos objetivos)
- A norma é destinada a atender às necessidades de uma ampla gama de partes interessadas, incluindo: os responsáveis pelo desenvolvimento da política de gestão de riscos no âmbito de suas organizações, os responsáveis por assegurar que os riscos são eficazmente gerenciados na organização como um todo ou em uma área, atividade ou projetos específicos, os que precisam avaliar a eficácia de uma organização em gerenciar riscos e os desenvolvedores de normas, guias.

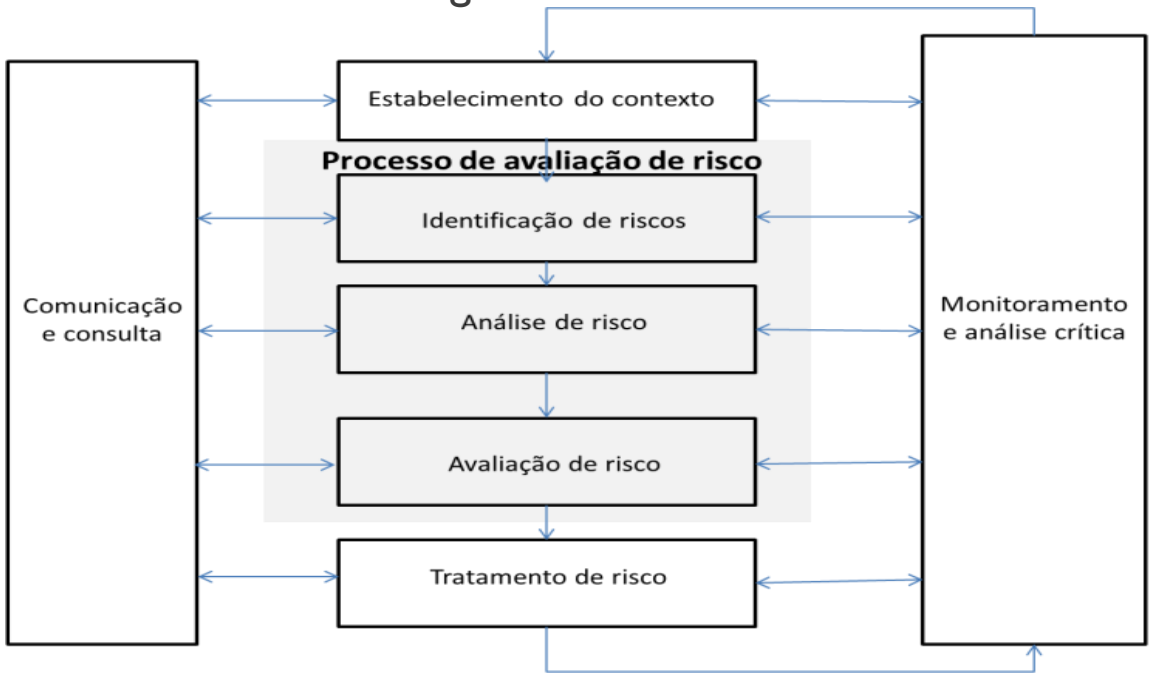
Modelo de causa de acidente - Queijo Suiço



Sucessivas camadas de defesas, barreiras e proteções

ABNT NBR ISO 3100:2009

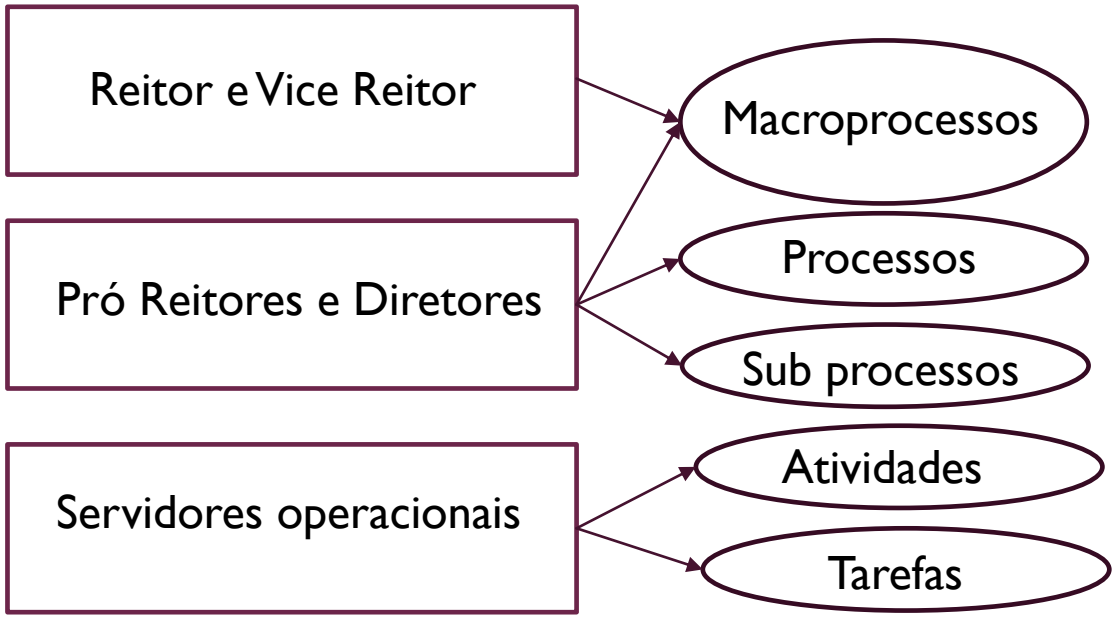
- As organizações gerenciam o risco, identificando-o, analisando-o, em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco. Ao longo de todo este processo, elas comunicam e consultam as partes interessadas e monitoram e analisam criticamente o risco e os controles que o modificam, a fim de assegurar que nenhum tratamento de risco adicional seja requerido. A norma descreve este processo sistemático e lógico em detalhes.

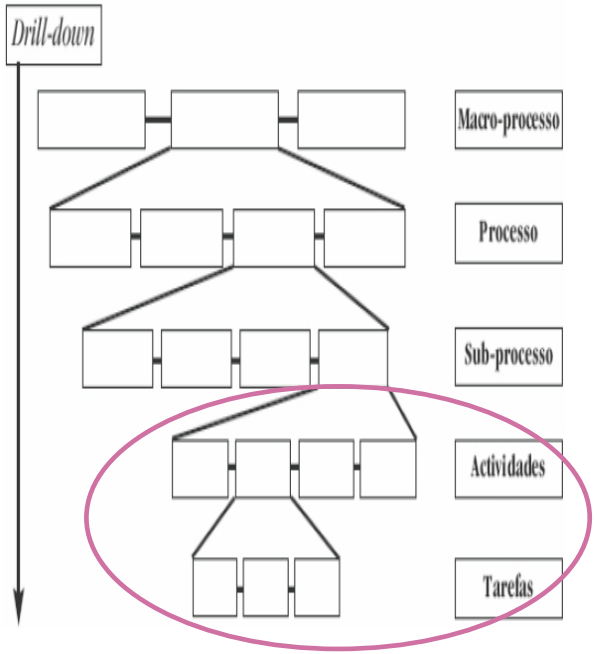


Fonte: ABNT NBR ISO 3100

ISO 31010:2009 TÉCNICAS PARA O PROCESSO DE AVALIAÇÃO DE RISCOS

- Considerando os quatro tipos de riscos estabelecidos pela IN nº1: **operacional, legal, imagem e financeiro**
- Cada nível da Instituição deve ESTABELECER O CONTEXTO

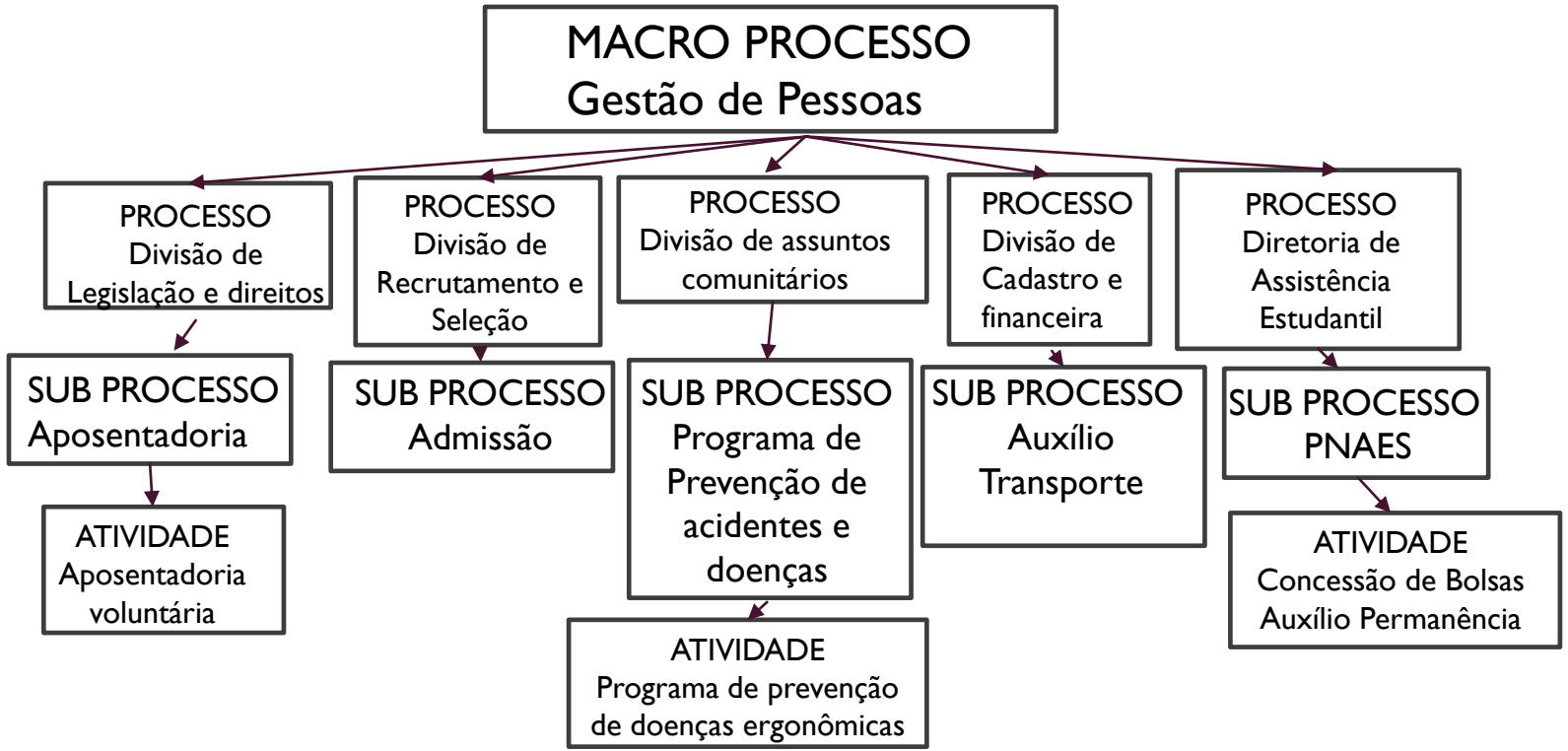


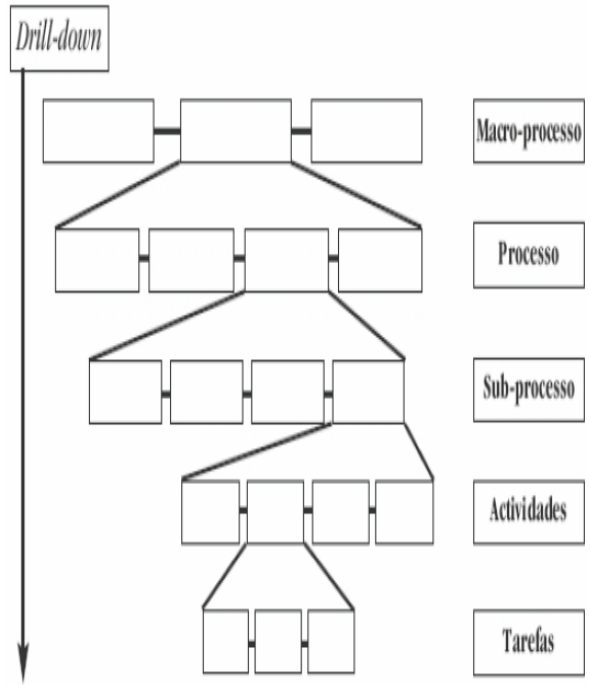


EXEMPLO: PRÓ REITORA DE GESTÃO DE PESSOAS

- O que devo me perguntar?

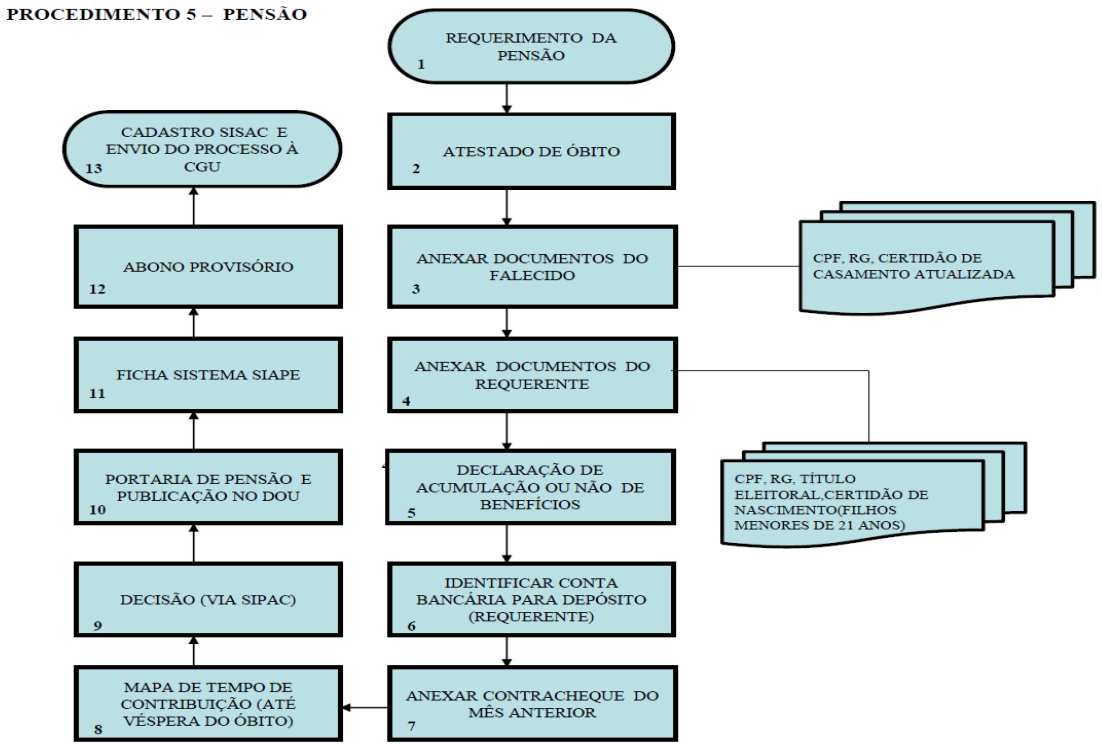
Quais os processos, sub processos, atividades e tarefas exercidas pelo meu setor que podem oferecer riscos?
RISCOS: legal, financeiro, operacional, de imagem à Universidade.

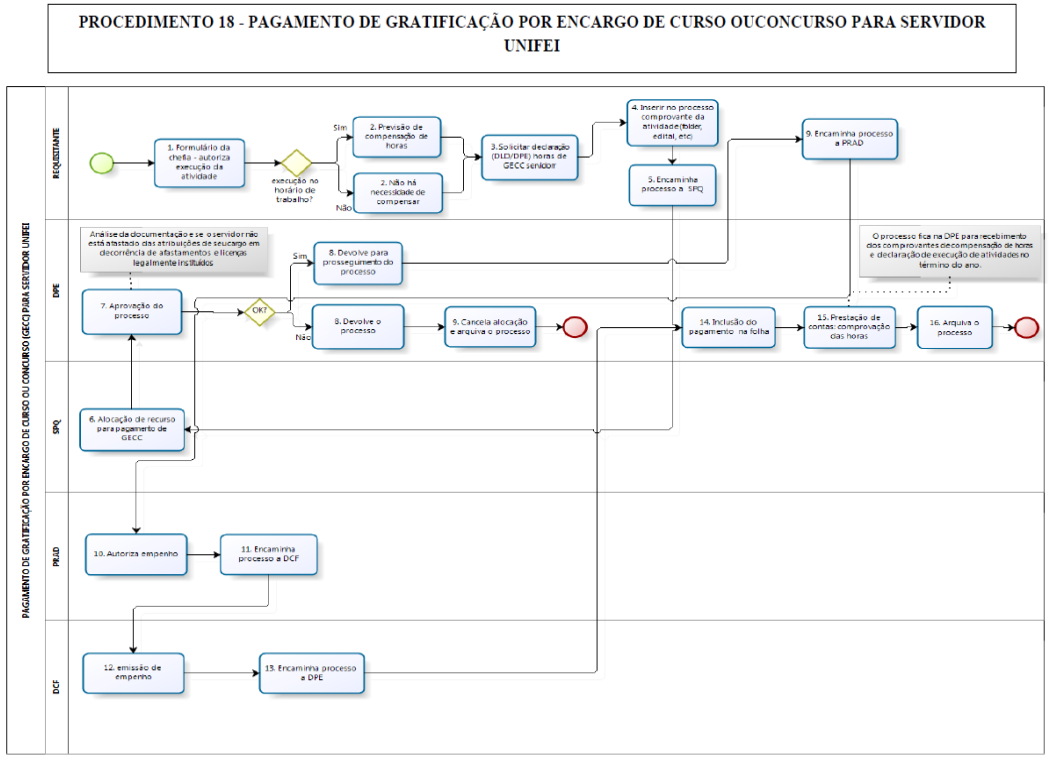




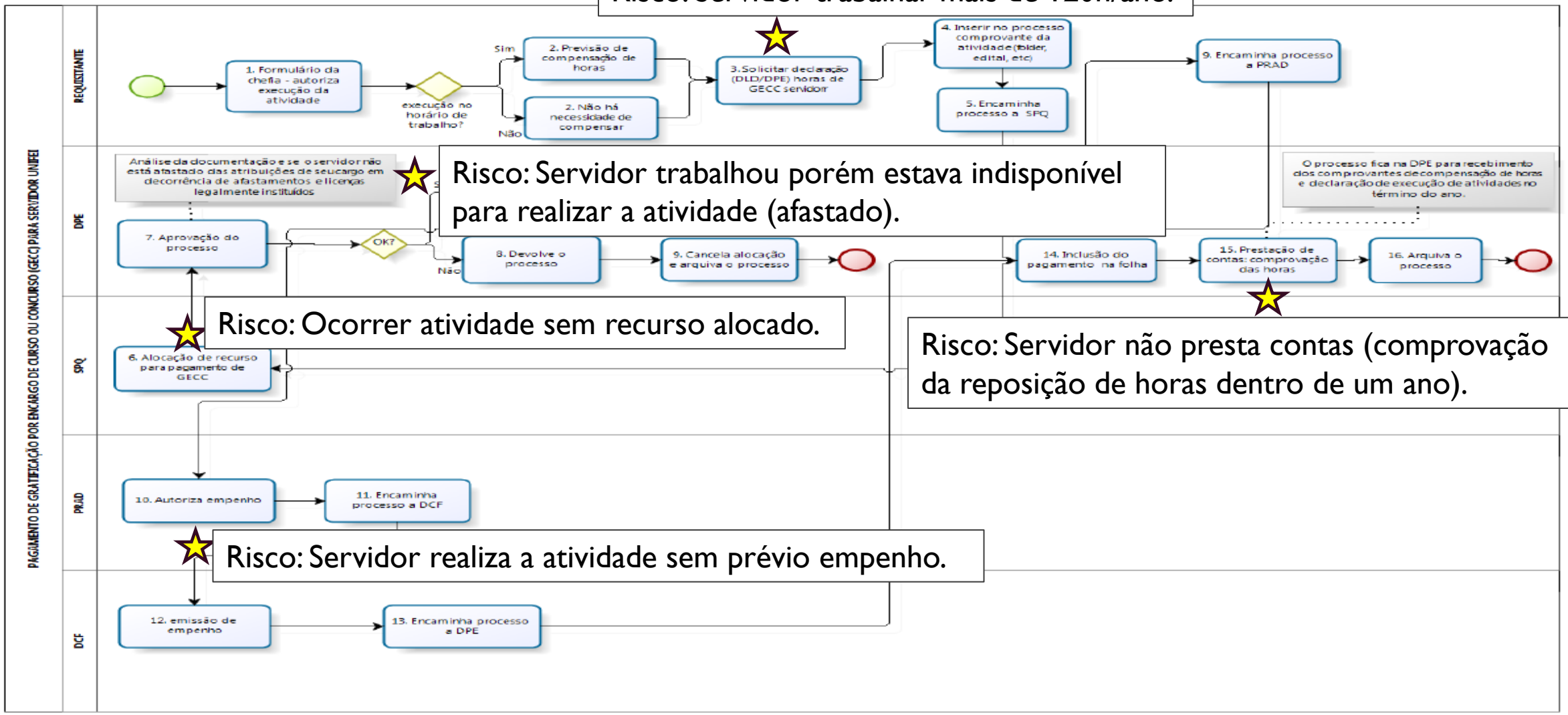
MAPEAMENTO DAS ATIVIDADES E TAREFAS

- Realizar o mapeamento das atividades executadas dentro de cada departamento;
- Forma Manual ou utilizando programas. Ex:





PROCEDIMENTO 18 - PAGAMENTO DE GRATIFICAÇÃO POR ENCARGO DE CURSO OUCONCURSO PARA SERVIDOR UNIFEI



Risco: Servidor trabalhar mais de 120h/ano.

Risco: Servidor trabalhou porém estava indisponível para realizar a atividade (afastado).

Risco: Ocorrer atividade sem recurso alocado.

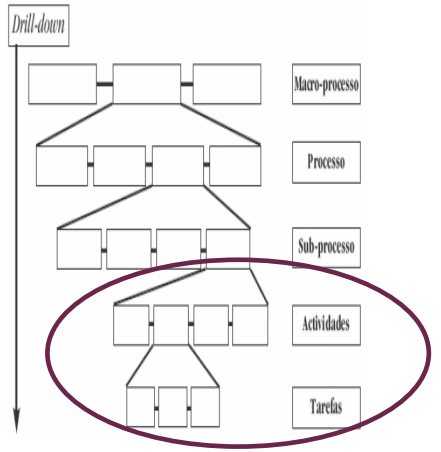
Risco: Servidor não presta contas (comprovação da reposição de horas dentro de um ano).

Risco: Servidor realiza a atividade sem prévio empenho.

IDENTIFICAR OS RISCOS

- MÉTODOS:
- Baseado em evidências – exemplo: dados históricos, achados de auditoria;
- Abordagem sistemática da equipe, perguntas entre a equipe;
- Técnicas de raciocínio indutivo- *What-if*
- Técnicas de apoio – *Brainstorming*
- Quem são as pessoas mais capazes de identificar os riscos dentro das atividades, tarefas ou processos em que atuam diretamente?

Alta gerência? Diretores? Ou servidores operacionais?



EXEMPLO:

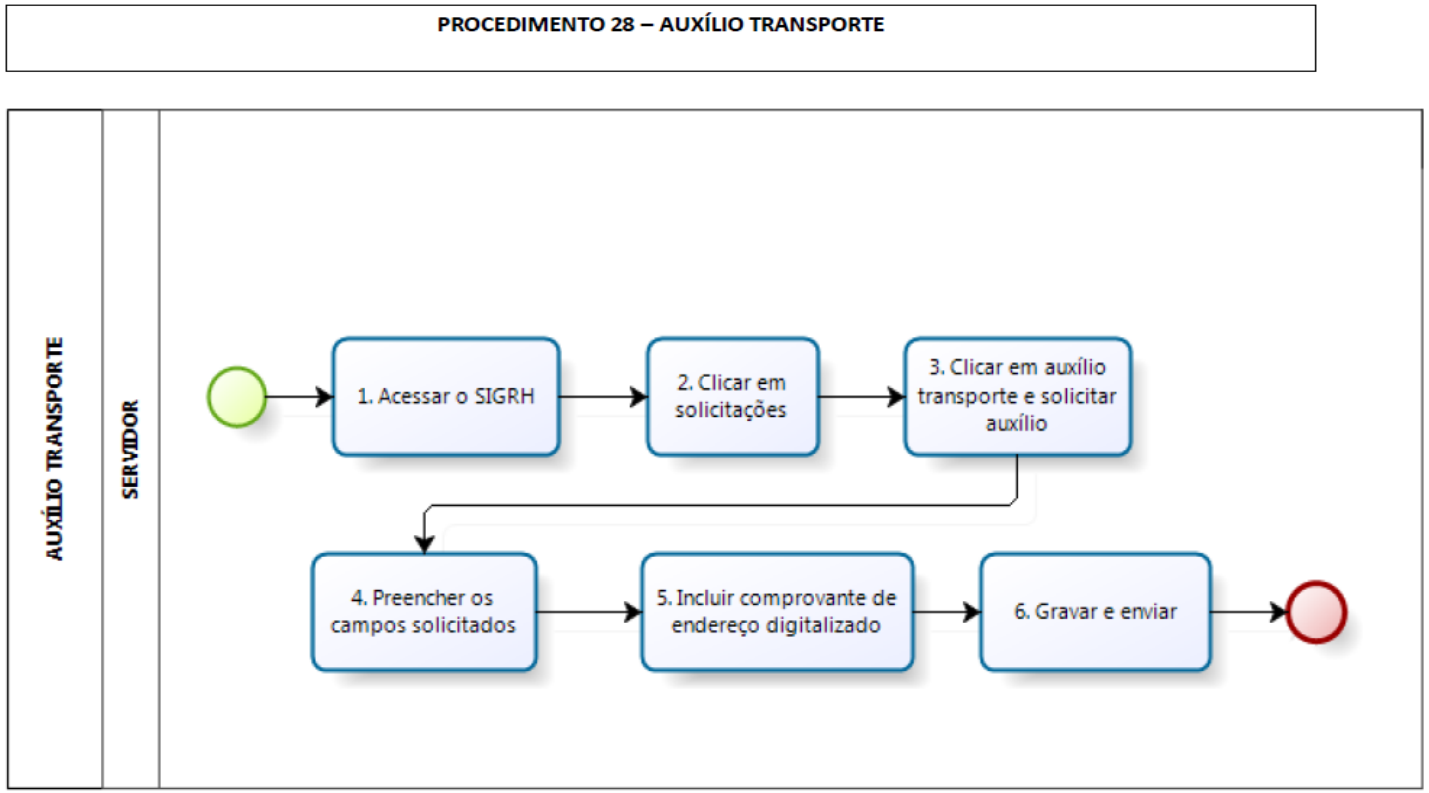
- Método evidências: Quais as principais constatações sobre este procedimento?

- Endereço informado no sistema diferente do comprovante de residência digitalizado;
- Comprovante de residência em nome de terceiros sem comprovação do vínculo;

- Técnica *what-if:*

- E se a pessoa preencher errado os campos solicitados?
- E se a pessoa não incluir o comprovante de endereço?
- E se...

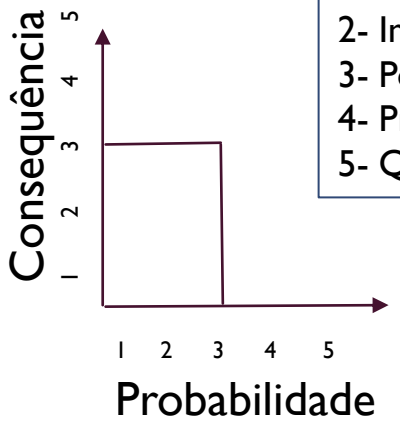
- *Braintorming:* reúne a equipe responsável e colocam as ideias de "o que pode dar errado"? O que seria um risco neste procedimento?



AVALIAÇÃO DOS RISCOS

- Trata-se de entender o risco.
- Estabelecer consequências e as probabilidades para determinar o nível do risco.
- Exemplo:

- Evento 1: Informar um endereço e anexar no sistema o comprovante com outro endereço.
- Risco Financeiro (pagamento indevido?) e risco operacional (falha no controle)



<u>Probabilidade</u>
1- Raro
2- Improvável
3- Possível
4- Provável
5- Quase certo

<u>Consequência</u>
1- Desprezível
2- Menor
3- Moderada
4- Maior
5- Catastrófica

E- Risco Extremo – ação imediata
A- Risco Alto – ação alta gerência
M- Risco Moderado – definir responsabilidade gerencial
B- Risco Baixo – manter práticas e procedimentos

Matriz qualitativa de riscos

Proba. \ Cons.	Desprezível	Menor	Moderada	Maior	Catastrófica
Quase Certo	A	A	E	E	E
Provável	M	A	A	E	E
Possível	B	M	A	E	E
Improvável	B	B	M	A	E
Raro	B	B	B	A	A

ANÁLISE DOS RISCOS

- Analisar se para cada evento encontrado:
- Os controles existentes são capazes de evitar que os riscos identificados ocorram?
- Analisar as consequências: alta ou baixa?
- Análise e estimativa da probabilidade. (dados históricos, opinião de especialistas)

EXEMPLO

- Análise da concessão do auxílio transporte para servidor que informa endereço divergente do anexado. Risco financeiro (pagamento indevido) e operacional (falha no controle)
- Os controles foram suficientes para identificar esta falha? NÃO
- A avaliação (cons. X prob.) foi de nível de RISCO ALTO (Matriz) que indica que devem ser tomadas as providências pela gerência;

E- Risco Extremo – ação imediata
A- Risco Alto – ação alta gerência
M- Risco Moderado – definir responsabilidade gerencial
B- Risco Baixo – manter práticas e procedimentos

APETITE AO RISCO = o quanto o gestor está disposto a assumir o risco.

		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito Alto	Médio 5	Elevado 10	Extremamente elevado 15	Extremamente elevado 20	Extremamente elevado 25
	Alto	Médio 4	Elevado 8	Elevado 12	Extremamente elevado 16	Extremamente elevado 20
	Médio	Médio 3	Elevado 6	Elevado 9	Elevado 12	Extremamente elevado 15
	Baixo	Baixo 2	Médio 4	Médio 6	Elevado 8	Elevado 10
	Muito Baixo	Baixo 1	Baixo 2	Médio 3	Médio 4	Médio 5

- Pessoas adequadas para analisar e avaliar são os Pró reitores e Diretores, além do dirigente máximo.
- Cada gestor e o dirigente máximo, em suas visões, devem definir seus critérios de análises e que tipo de ação deve ser tomada;

AÇÕES FUTURAS

- O risco precisa de tratamento?
- Qual a prioridade para o tratamento?

- Avaliar a decisão de tratamento do risco

Custo benefício de se assumir o risco x Custo benefício de implementar novos controles

Vale a pena tratar o risco, ou assumir a suas consequências?

QSP

VISÃO (PARCIAL) DO PROCESSO DE GESTÃO DE RISCOS *(segundo a ISO 31000)*

IDENTIFICAÇÃO **DO RISCO**

ANÁLISE e AVALIAÇÃO **DO RISCO**

TRATAMENTO **DO RISCO**

TRATAMENTOS (EXEMPLOS)

Risco: Pagamento indevido do aux. Transporte.

Causa: Aceite de documentação inadequada pelo sistema.

Fonte de risco: Deficiência no sistema operacional SIG de reconhecimento do documento adequado.

TRATAMENTOS

1- Remover a fonte de risco (Fonte: Sistema SIG deficiente. Não utilizar mais o sistema para conceder o auxílio)

2- Evitar o risco (Decisão de não iniciar ou descontinuar a atividade que dá origem ao risco – Não conceder mais o auxilio transporte)

3- Alterar a probabilidade = ação preventiva (Estabelecer mais controle: Orientar formalmente os solicitantes quanto à atenção no preenchimento dos dados no sistema o e comprovante que deve ser anexado; Realizar dupla checagem pelos servidores do DPE na documentação anexada no sistema)

4- Alterar a consequência = ação corretiva/diminuir o efeito (pagamento indevido– pedir restituição do valor pago indevidamente)

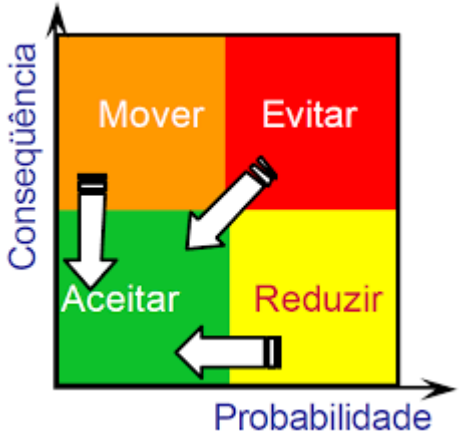
5- Transferir o risco – terceirização (Seguros)

6- Reter o risco- assumir. (Não estabelecer tratamento algum, assumir o risco quando mais vantajoso)

TRATAMENTO: PROBABILIDADE X CONSEQUÊNCIA

Alterar apenas a Probabilidade

		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito Alto	Médio 5	Elevado 10	Extremamente elevado 15	Extremamente elevado 20	Extremamente elevado 25
	Alto	Médio 4	Elevado 8	Elevado 12	Extremamente elevado 16	Extremamente elevado 20
	Médio	Médio 3	6	Elevado 9	Elevado 12	Extremamente elevado 15
	Baixo	Baixo 2	Médio 4	Médio 6	Elevado 8	Elevado 10
	Muito Baixo	Baixo 1	Baixo 2	Médio 3		



Alterar apenas a Consequência/Impacto

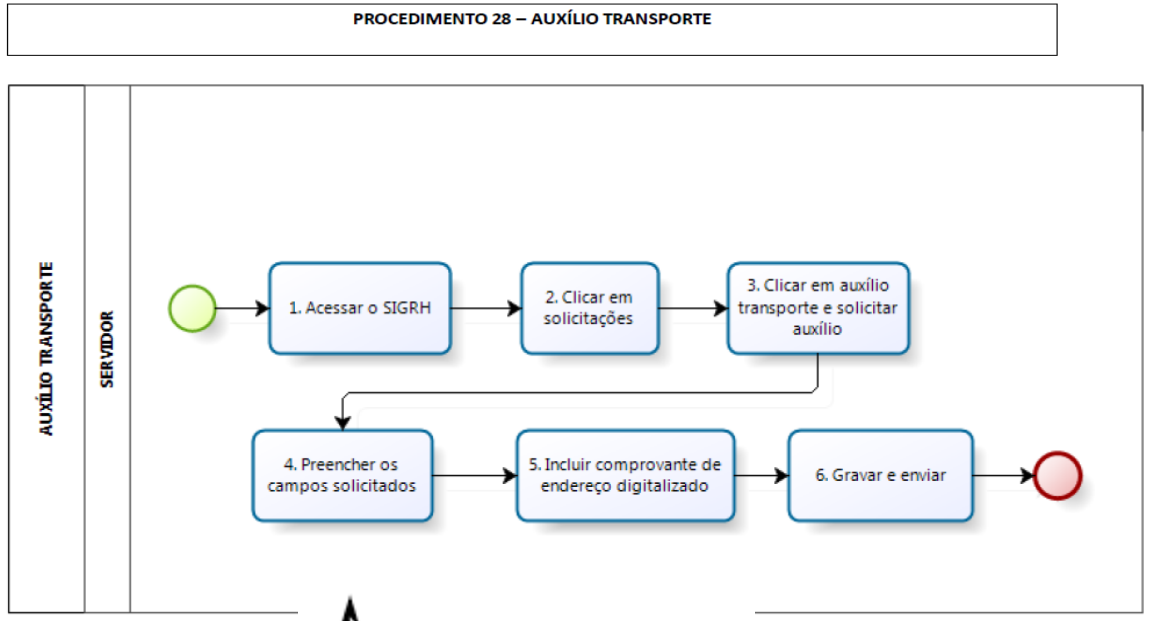
		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito Alto	Médio 5	Elevado 10	Extremamente elevado 15	Extremamente elevado 20	Extremamente elevado 25
	Alto	Médio 4	Elevado 8	Elevado 12	Extremamente elevado 16	Extremamente elevado 20
	Médio	Médio 3	Elevado 6	Elevado 9	Elevado 12	Extremamente elevado 15
	Baixo	Baixo 2	Médio 4	Médio 6	Elevado 8	Elevado 10
	Muito Baixo		Baixo 2	Médio 3	Médio 4	Médio 5

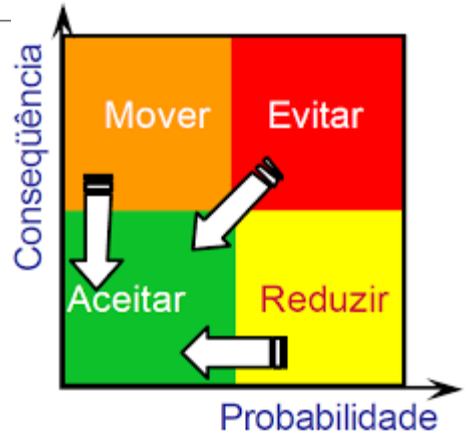
Alterar a Consequência/Impacto e a probabilidade

		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito Alto	Médio 5	Elevado 10	Extremamente elevado 15	Extremamente elevado 20	Extremamente elevado 25
	Alto	Médio 4	Elevado 8	Elevado 12	Extremamente elevado 16	Extremamente elevado 20
	Médio	Médio 3	Elevado 6	Elevado 9	Elevado 12	Extremamente elevado 15
	Baixo	Baixo 2	Mé	Médio 6	Elevado 8	Elevado 10
	Muito Baixo	Baixo 1	Baixo 2	Médio 3	Médio 4	Médio 5

EXEMPLO- TRATAMENTO

- O gestor entendeu que este risco (financeiro e operacional) deve receber um tratamento;
- Qual?
- Alterar a probabilidade e a consequência para que se torne um risco aceitável.
- Alterar a Probabilidade: Implementar novos controles; (verificação manual de cada comprovante do sistema ou implantar reconhecimento automático de imagem dos documentos) E configurar o sistema para não deixar campos de informação em branco e sem anexo;
- Alterar a consequência: Exigir restituição do valor recebido indevidamente;





MONITORAMENTO E ANÁLISE CRÍTICA

- Envolvem checagens e vigilâncias regulares. (Garantir que os controles sejam eficazes e eficientes nos procedimentos);
- Podem ser periódicos ou acontecer em resposta a um fato específico;
- Analisar os eventos, mudanças, tendências, sucessos e fracassos e aprender com eles;
- Detectar mudanças no contexto interno e externo, o que pode trazer alterações nos critérios de riscos e nos seus tratamentos.
- Obs.: O monitoramento manual pode se tornar muito trabalhoso ou inviável. O ideal seria o monitoramento por sistemas de informação, mas depende de sua disponibilidade.

MONITORAMENTO E ANÁLISE CRÍTICA

- Podem ser aplicados em todo o processo de gestão de riscos, no controle ou no risco. (Identificar mudanças no nível do desempenho esperado)
- Exemplo:
- Monitoramento aplicado ao risco: De acordo com o nível do risco, Alto ou Muito alto, devem ser monitorados periodicamente, por exemplo mensalmente, de acordo com a vontade do gestor.
- Monitoramento aplicado ao controle: A conferência do endereço do servidor feita por reconhecimento automático de imagem, e não mais manualmente por um outro servidor, altera o nível de desempenho deste controle . Quando a checagem for realizada de forma automática trará mais segurança e menores chances de ocorrerem erros.
- Monitoramento em todo o processo de gestão de risco: Utilizar sistema integrado capaz de indicar ao gestor, durante a execução de seus procedimentos, todos os potenciais riscos e os possíveis tratamentos para este. Sistema SIG Módulo Gestão de Riscos- sendo desenvolvido/ a ser implantado. (UFRN)

RESUMINDO:

CURSOS

ABNT Cursos

ABNT NBR ISO 31000 – Gestão de Riscos – Princípios e Diretrizes

QSP

ISO 31000, ISO Guia 73 e ISO/IEC 31010
Conheça as atividades pioneiras do QSP relacionadas às novas referências mundiais para a Gestão de Riscos
Outubro/2013

Curso Pioneiro e Exclusivo do QSP
Capacitação em Gestão de Riscos e Auditoria Baseada em Riscos

Para mais informações, acesse: http://www.qsp.org.br/capacitacao_gr.shtml

---

Mais um Curso Pioneiro e Exclusivo do QSP
Seleção de Ferramentas e Técnicas de Risk Assessment

Para mais informações, acesse: http://www.qsp.org.br/curso_risk.shtml

---

AÇÕES CONJUNTAS (IFES)

- Capacitações
- Estudos de casos
- Compartilhar mapas de riscos e processos
- *Benchmark* (identificação de riscos em comum para servir de comparação)
- Ação conjunta com a UFRN na gestão de riscos (Modelagem de Sistema)

REFERÊNCIAS

- SILVA, Bruno. **Modelo de Gestão de Riscos em Instituições Federais de Ensino Superior (IFES).** UFRN: Natal, 2016.

- ABNT NBR ISO 31000:2009. **Gestão de riscos- Princípios e diretrizes**. Associação Brasileira de Normas Técnicas- ABNT. Rio de janeiro, 2009.

- ABNT NBR ISO/IEC 31010. **Gestão de riscos- técnicas para o processo de avaliação de riscos**. Associação Brasileira de Normas Técnicas- ABNT. Rio de janeiro, 2012.

- Júnior, Joacir Araújo Machado**. ISO 31010:2009 – Avaliação de Riscos – Seleção de Ferramentas e Tácnicas de *Risk Assessment***. QSP- Centro da Qualidade, Segurança e Produtividade para o Brasil e América Latina: São Paulo, 2016.