interlocus
aprendizagem e colaboração

MINISTÉRIO DA SAÚDE

AUDITORIA INTERNA COM FOCO EM AVALIAÇÃO DE RISCOS

Salvatore Palumbo

Curitiba
Novembro 2015

Agenda

1. Apresentando-nos
2. Apresentando o objetivo e a estrutura do curso
3. Descrevendo a dinâmica das atividades

Apresentando-nos

- Seu nome
- Com que você trabalha?
- O que você espera do curso?

Objetivo geral do curso

- Os participantes, ao final do curso, deverão ser capazes de aplicar padrões e procedimentos de auditoria às fases analítica, operativa e de relatório que contribuem para a qualidade das auditorias realizadas no âmbito do Sistema Único de Saúde (SUS).

Estrutura do curso

Módulo 0 - RISCOS E CONTROLES NA ADMINISTRAÇÃO PÚBLICA

Módulo 1 - INTRODUÇÃO À AUDITORIA DO SUS

Módulo 2 - PROGRAMAÇÃO DE AUDITORIA

Módulo 3 - FASE ANALÍTICA DA AUDITORIA

Módulo 4 - FASE OPERATIVA DA AUDITORIA

Módulo 5 - FASE DE RELATÓRIO

Estrutura do curso

Módulo 0

RISCOS E CONTROLES NA ADMINISTRAÇÃO PÚBLICA

0.1 Identificação e avaliação de riscos

0.2 Controle Interno e suas limitações

Estrutura do curso

Módulo 1

INTRODUÇÃO À AUDITORIA DO SUS

- 1.1 Processo de auditoria no SUS
- 1.2 Princípios éticos e profissionais do auditor

Módulo 2

PROGRAMAÇÃO DE AUDITORIA

- 2.1 Interpretação da demanda
- 2.2 Elaboração da tarefa

Estrutura do curso

Módulo 3

FASE ANALÍTICA DA AUDITORIA

- 3.1 Visão geral da fase analítica
- 3.2 Uso de matrizes de coleta e de análise e informações em auditoria
- 3.3 Procedimentos de coleta e de análise de informações
- 3.4 Validação das matrizes de coleta e de análise e informações
- 3.5 Relatório analítico

Estrutura do curso

Módulo 4
FASE OPERATIVA DA AUDITORIA

- 4.1 Trabalho de campo
- 4.2 Evidências e constatações
- 4.3 Matriz de constatações
- 4.4 Relatório preliminar

Módulo 5
RELATÓRIO DE AUDITORIA

- 5.1 Qualidade do relatório de auditoria
- 5.2 Encerramento da auditoria

Estrutura do curso

Módulo 0 - RISCOS E CONTROLES NA ADMINISTRAÇÃO PÚBLICA

Módulo 1 - INTRODUÇÃO À AUDITORIA DO SUS

Módulo 2 - PROGRAMAÇÃO DE AUDITORIA

Módulo 3 - FASE ANALÍTICA DA AUDITORIA

Módulo 4 - FASE OPERATIVA DA AUDITORIA

Módulo 5 - FASE DE RELATÓRIO

Módulo 0

RISCOS E CONTROLES NA ADMINISTRAÇÃO PÚBLICA

Ao final deste módulo, os participantes deverão ser capazes de aplicar método para identificar e avaliar riscos e controles, bem como de reconhecer limitações de um sistema de controle interno.

Sessão 0.1

Identificação e avaliação de riscos e controles

Os participantes deverão ser capazes, ao final da sessão, de conceituar risco e de aplicar método para identificar e avaliar riscos e controles que afetam o setor público.

Riscos estão por toda parte!


150

Quais os riscos envolvidos?

O QUE ESSES RISCOS TÊM EM COMUM?

- Alguém se ferir
- Haver discussão
- A bola furar
- Alguém ser posto à margem do jogo e ficar chateado
- Serem expulsos da quadra por “valentões”
- Chover

O QUE ESSES RISCOS TÊM EM COMUM?

- Eventos futuros
- Eventos incertos
- Afetam os objetivos dos envolvidos

Avaliação dos riscos

Riscos são avaliados em termos de probabilidade de ocorrência e de impacto nos objetivos.

Objetivo	Risco	Probabilidade	Impacto
Manter a integridade física	Alguém se ferir	Baixa	Médio
Manter a coesão do grupo	Haver discussão	Alta	Médio
	Ser posto à margem do jogo	Média	Médio
Continuar jogando	Bola furar	Muito baixa	Muito alto
	Serem expulsos da quadra	Baixa	Muito alto
	Chover	Muito baixa	Médio

Conceitos de Risco

COSO

- Possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos.

TCU

- Possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades.

Riscos acompanham objetivos

OBJETIVOS	RISCOS
Reduzir a carência de médicos em cidades distantes dos grandes centros por meio de programa de incentivo	Baixa adesão ao programa
Reduzir o nível de falhas e irregula-ridades em procedimentos adminis-trativos por meio de capacitação	Contingenciamento de recursos previstos para ações de capacitação
Oferecer transporte público urbano de qualidade	Ônibus quebrar durante o transporte de passageiros

Vamos trabalhar

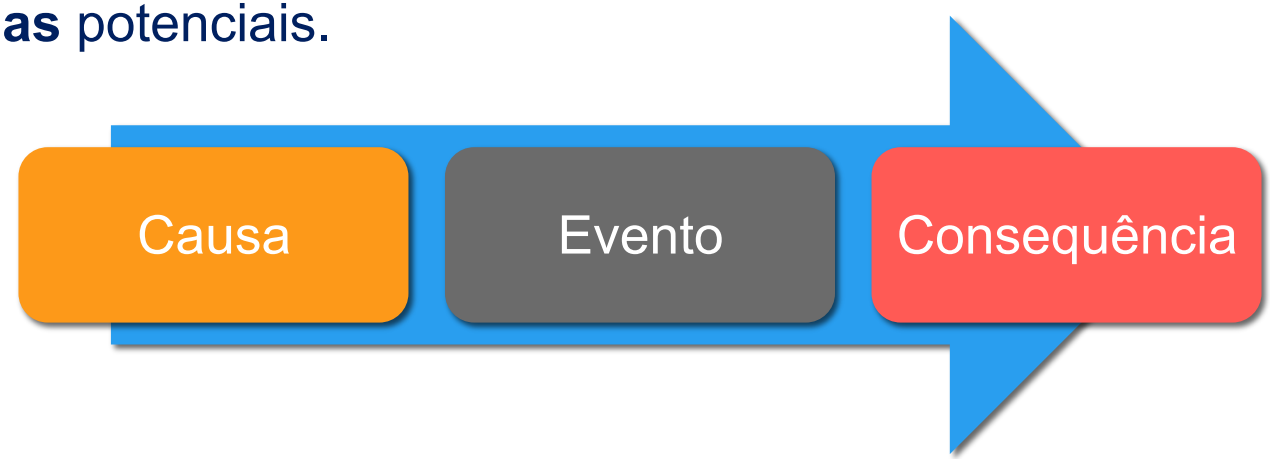
1. O SAMU 192 tem por missão prestar atendimento pré-hospitalar de urgência de excelência à população. Isso inclui atender os chamados no menor tempo possível e garantir o acesso do paciente à unidade de saúde apropriada.

2. Levantem, em duplas, uma lista de três a cinco riscos que podem impactar negativamente a missão do SAMU 192.

Identificação de Riscos

Conceito de identificação de riscos

- **Processo de busca, reconhecimento e descrição de riscos (ISO 31000)**
- Envolve a identificação de **fontes** de risco, **eventos**, suas **causas** e suas **consequências** potenciais.



- Um princípio que não pode ser esquecido na identificação de riscos é que **eles se relacionam com os objetivos da organização, do processo, do projeto etc.**
- A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas informadas, especialistas e partes interessadas.

Por que identificar riscos?

- **Se**
  - riscos são eventos que podem impactar os objetivos da organização e
  - importa assegurar que objetivos sejam alcançados
- **Então**
  - deve-se adotar medidas para lidar com riscos
- **Porém**
  - como **não se pode lidar com aquilo que não se conhece**, riscos devem ser identificados!

Como identificar riscos?

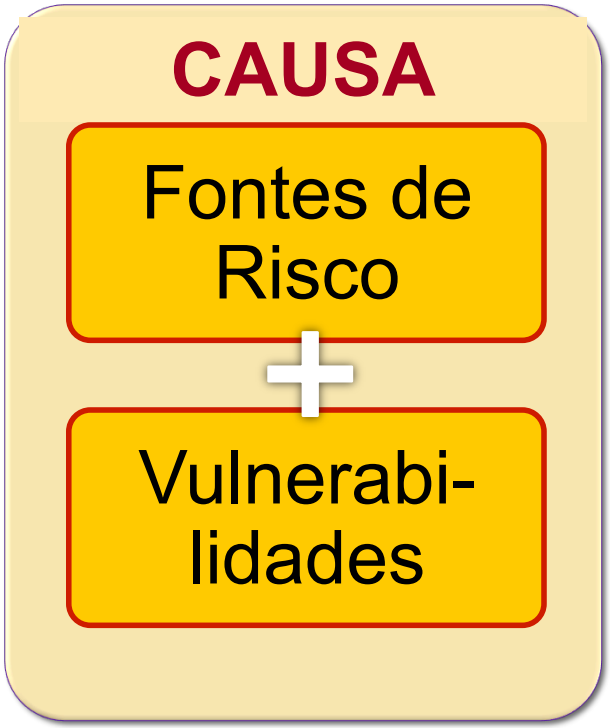
- A identificação de riscos requer:
  - ✓um objetivo a ser alcançado claramente definido;
  - ✓identificação dos eventos que podem impactar esse objetivo;
  - ✓suas causas (ou fatores de risco); e
  - ✓suas consequências em termos de impactos no objetivo

- Uma maneira de representar graficamente um risco é por meio da técnica *bow tie* (gravata borboleta), a seguir.

Representação de um risco usando bow tie

Causas do risco

- Condições que dão origem à possibilidade de um evento acontecer.
- Causas também são chamadas **fatores de riscos** e podem ter origem no ambiente externo ou interno à organização.



Causa = fonte + vulnerabilidade

- **Fonte de risco:** elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco:
  - pessoas
  - processos
  - sistemas
  - infra-estrutura física/organizacional
  - tecnologia [de produto ou de produção]
  - eventos externos (não gerenciáveis)
- **Vulnerabilidade:** inexistências, inadequações ou deficiências em uma fonte de risco.

Exemplos de Causas

Da Fonte

- **Pessoas**

Vulnerabilidades

- Em número insuficiente
- Sem capacitação
- Perfil inadequado
- Desmotivadas
- ...

Exemplos de Causas

Da Fonte

- **Processos**

Vulnerabilidades

- Mal concebidos (fluxo, desenho)
- Sem manuais ou instruções formalizadas (procedimentos)
- Ausência de segregação de funções
- ...

Exemplos de Causas

Da Fonte

- **Sistemas**

Vulnerabilidades

- Obsoletos
- Sem integração
- Sem manuais de operação
- Inexistência de controles de acesso lógico / *backups*
- ...

Exemplos de Causas

Da Fonte

- **Estrutura organizacional**

Vulnerabilidades

- Falta de clareza quanto à funções e responsabilidades
- Deficiências nos fluxos de informação e comunicação
- Centralização de responsabilidades
- Delegações exorbitantes
- ...

Exemplos de Causas

Da Fonte

- **Infraestrutura física**

Vulnerabilidades

- Localização inadequada
- Instalações ou leiaute inadequados
- Inexistência de controles de acesso físico
- ...

Exemplos de Causas

Da Fonte

- **Tecnologia** (de produto ou de produção)

Vulnerabilidades

- Técnica de produção ultrapassada / produto obsoleto
- Inexistência de investimentos em pesquisa e desenvolvimento
- Tecnologia sem proteção de patentes
- Processo produtivo (tecnologia) sem proteção contra espionagem
- ...

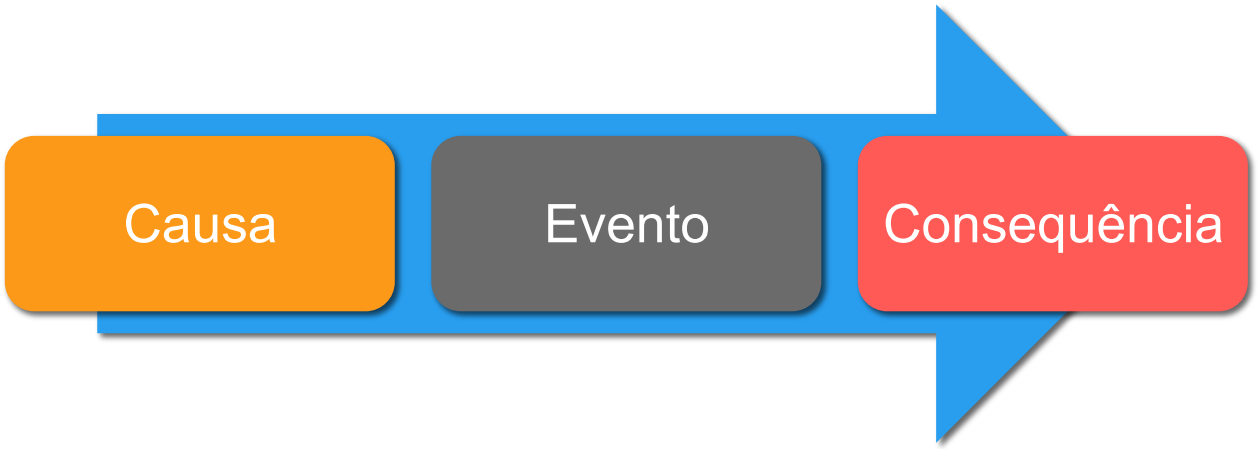
Consequências do risco

- Resultados de um evento sobre os objetivos.
- Exemplos:
  - Indisponibilidade de sistema gera atraso no atendimento de pacientes.
  - Desabamento de viaduto leva a perda de vidas e prejuízos materiais.

Dimensões de um objetivo impactadas

Sintaxe para descrição de um risco

Devido a <CAUSA/FONTE DE RISCO>, poderá acontecer <EVENTO>, o que poderá levar a <IMPACTO, CONSEQUÊNCIA, EFEITO> impactando o/a <DIMENSÃO DE OBJETIVO IMPACTADA>.



Descrição de um risco usando a sintaxe

- **Objetivo da empresa:** apresentar propostas para licitações até as datas fixadas em editais (depende de cotações de preços de seus fornecedores).
- **Causa/Fonte:** não entrega em tempo hábil de cotações de preços por parte de fornecedores.
- **Evento:** não participação da empresa em licitações.
- **Consequência/Impacto:** interrupção de atividades causando impacto no fluxo de caixa.
- **Descrição do risco:** Devido a não entrega em tempo de cotações de preços por parte de fornecedores, poderá acontecer a não participação da empresa em licitações, o que poderá levar a interrupção de atividades, impactando o fluxo de caixa da entidade.

Processo de identificação e avaliação de riscos

- Deve envolver a equipe de modo a desenvolver e manter sentimento de propriedade e responsabilidade pelos riscos e pelas ações de tratamento.

Ferramentas e técnicas

- Brainstorming
- Entrevistas
- Análise SWOT
- Análise de dados históricos
- Opiniões de especialistas e pessoas informadas
- Necessidades das partes interessadas (*stakeholders*)
- Mapa de processo

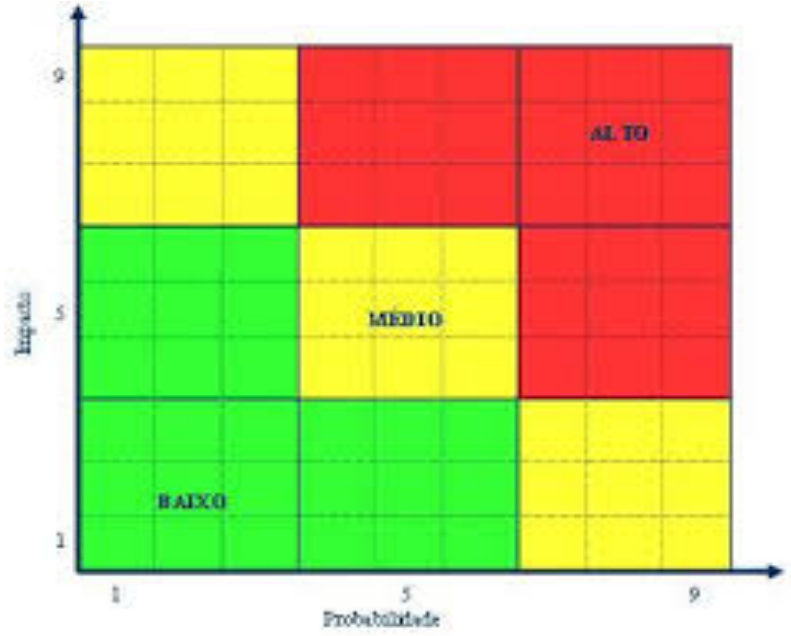
Registro de Riscos

Função/ Atividade	Compilado por	Data
Objetivo	Analisado por	Data

Riscos Identificados			Avaliação			Controles Existentes		Risco Residual	Recomendação	
Eventos	**Causas**	**Consequências**	**Prob.**	**Impacto**	**Nível**	**Descrição**	**Eficácia**		**Tratar risco**	**Prior.**

Vamos trabalhar na Identificação de riscos

- Em situações reais, a identificação e a avaliação de riscos devem ser feitas separadamente. Primeiro identificam-se todos os riscos para depois realizar a sua avaliação.
- Em grupos de 3 a 4 pessoas, preencham, no **Registro de Riscos**, apenas a coluna 'Riscos Identificados', identificando cada risco com os seguintes componentes:
  - ✓ O evento que pode acontecer e ter um impacto nos objetivos;
  - ✓ A causa que pode levar o evento a acontecer, expressando a vulnerabilidade e a fonte;
  - ✓ A consequência (ou impacto) do risco nos objetivos.



Avaliação de Riscos

Por que avaliar riscos?

- **Porque**
  - a organização está exposta a uma grande quantidade de riscos e
  - **não existem recursos** (tempo, dinheiro, pessoas) para lidar com todos os riscos identificados.
- **Então**
  - deve-se concentrar recursos para lidar com os riscos que mais podem impactar (riscos-chave) os objetivos da organização, do processo, do projeto.

Avaliação de um risco

- Um risco é avaliado em termos de probabilidade de ocorrência e de impacto sobre os objetivos.

Nível do Risco = Probabilidade x Impacto

- Quanto maior a probabilidade e maior o impacto, maior é o nível do risco.

Critérios para avaliação de riscos

- Para determinar os níveis de risco, é preciso definir **escalas** para estimar a probabilidade e o impacto, bem como estabelecer quando a combinação desses dois fatores representa um risco baixo, médio ou alto.
- A seguir, são exemplificadas escalas qualitativas para auxiliar na estimativa de probabilidades e impactos de eventos, bem como uma matriz Impacto x Probabilidade, que define níveis de risco decorrentes da combinação desses dois fatores.

Escala de probabilidades

Descritor	Descrição	Nível
Muito Baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Não há histórico de sua ocorrência.	1
Baixa	Evento casual, inesperado. Apesar de raro, há histórico conhecido de sua de ocorrência por parte dos principais gestores e operadores do processo.	2
Média	Evento esperado, que se reproduz com frequência reduzida. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo.	3
Alta	Evento usual, corriqueiro. Sua ocorrência habitual ou conhecida amplamente conhecida por parte de gestores e operadores do processo.	4
Muito Alta	Evento se reproduz muitas vezes, seguidamente, e interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo.	5

Escala de Impactos

Descritor	Descrição	Nível
Muito Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização com **impactos mínimos** nos objetivos de prazo, custo, qualidade, escopo ou imagem.	**1**
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos pequenos** nos objetivos de prazo, custo, qualidade, escopo ou imagem.	**2**
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando **impactos significativos, porém recuperáveis**, nos objetivos de prazo, custo, qualidade, escopo ou imagem.	**3**
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando **impactos de reversão muito difícil** nos objetivos de prazo, custo, qualidade, escopo ou imagem.	**4**
Muito Alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos irreversíveis** nos objetivos de prazo, custo, qualidade, escopo ou imagem.	**5**

Matriz Impacto x Probabilidade e Níveis de Risco

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
Impacto	5 Muito Alto	5	10	15	20	25
	4 Alto	4	8	12	16	20
	3 Médio	3	6	9	12	15
	2 Baixo	2	4	6	8	10
	1 Muito Baixo	1	2	3	4	5

Extremo

Alto

Médio

Baixo

Registro de Riscos

Função/ Atividade	Compilado por	Data
Objetivo	Analisado por	Data

Riscos Identificados			Avaliação			Controles Existentes		Risco Residual	Recomendação	
Eventos	**Causas**	**Consequências**	**Prob.**	**Impacto**	**Nível**	**Descrição**	**Eficácia**		**Tratar risco**	**Prior.**

Vamos trabalhar na Avaliação de riscos

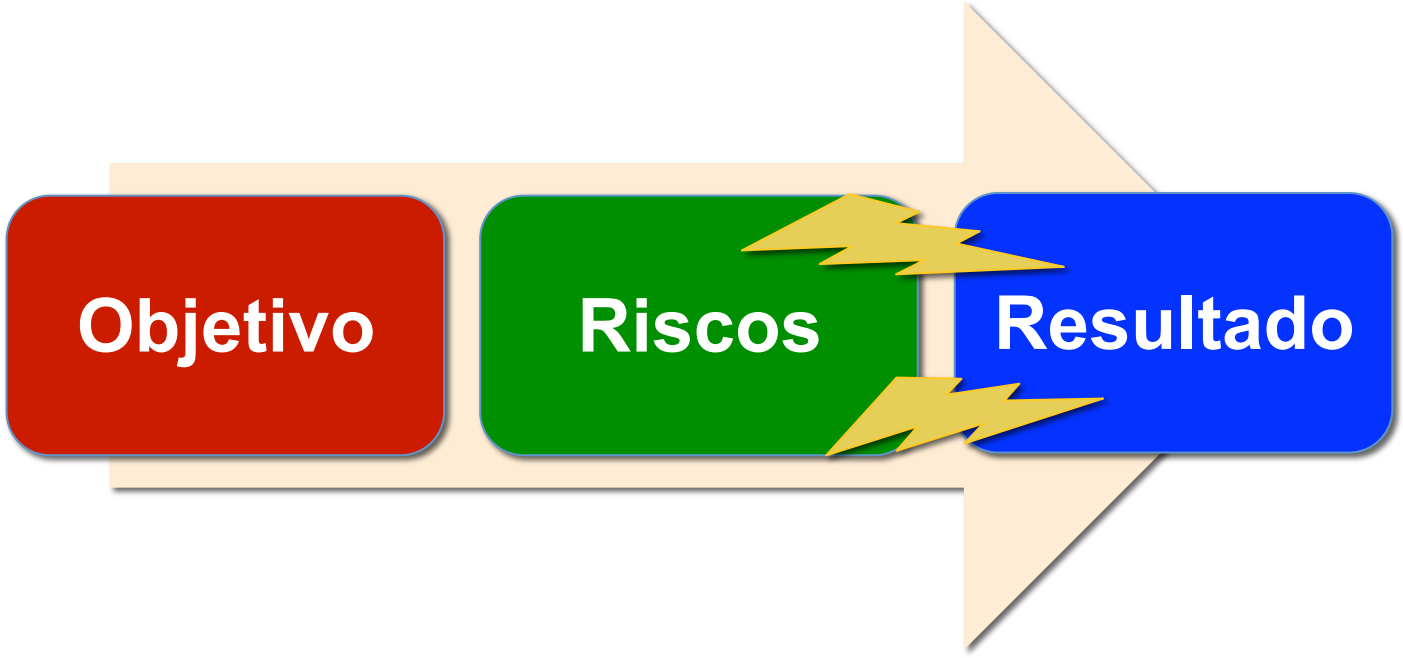
- Em grupos de 3 a 4 pessoas, preencham no **Registro de Riscos** a coluna ‘Avaliação’, tomando por base as escalas de probabilidade e impactos apresentadas:
  - ✓ Na coluna ‘Probabilidade’, indique o número (de 1 a 5) que melhor corresponda à descrição da probabilidade de ocorrência do risco (conforme Escala de Probabilidades).
  - ✓ Na coluna Impacto, proceda da mesma forma, seguindo a Escala de Impactos.
  - ✓ Na coluna ‘Nível’ (de risco inerente), indique o resultado da multiplicação dos números indicados nas duas colunas anteriores e escreva o nível (baixo, médio, alto ou extremo).

Objetivo estabelecido

Resultado alcançado

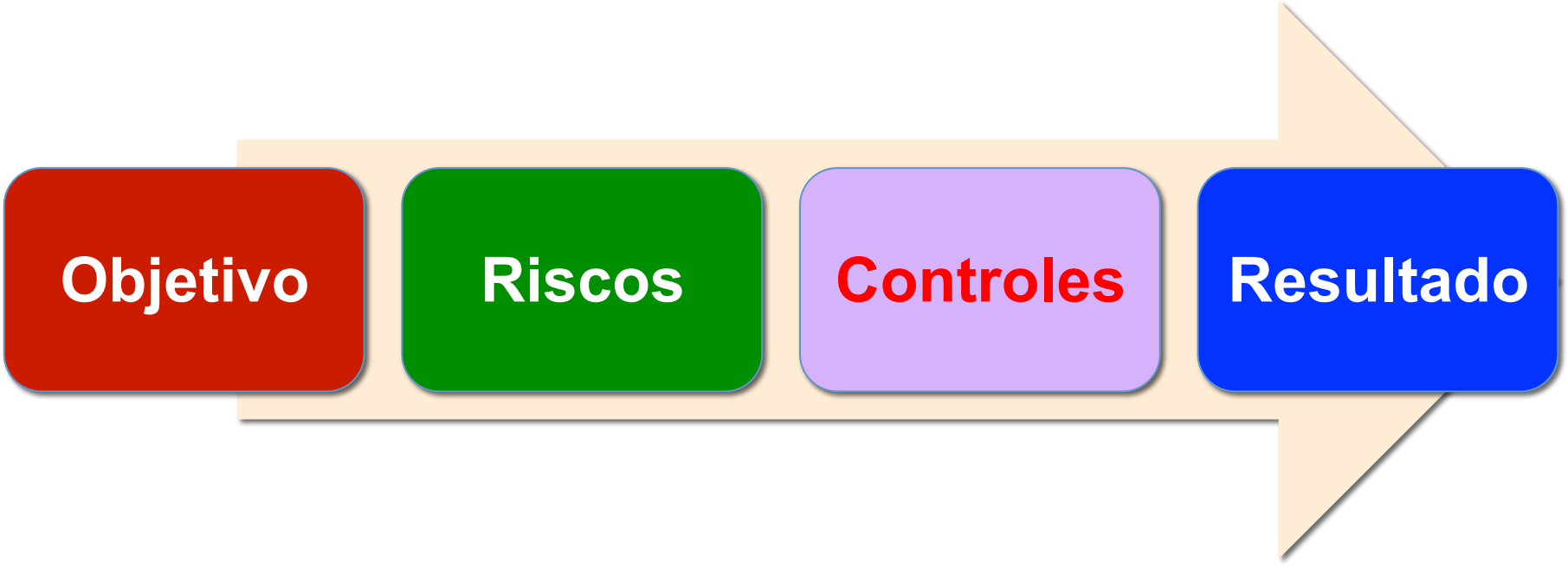
Como se pode aumentar a chance de que um objetivo estabelecido seja alcançado?

A incerteza dos riscos reflete-se em incerteza nos resultados!



Sem conhecer e atuar sobre os riscos envolvidos, pode haver consequências indesejadas.

Controles aumentam a previsibilidade do resultado ao atuarem sobre os riscos!

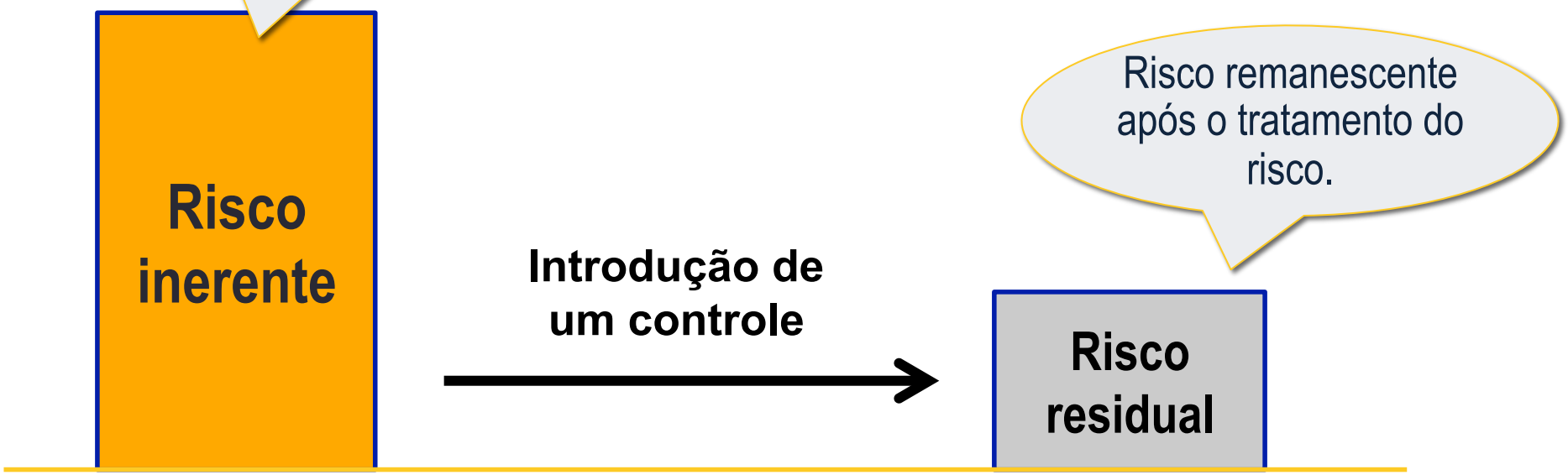


Mas, o que são controles?

Controle reduz nível do risco

Risco do negócio ou do processo antes de qualquer tratamento ou controle

Controle é uma política ou procedimento capaz de mitigar um risco.



Risco remanescente após o tratamento do risco.

Exemplos

Objetivos	Riscos	Controles
Efetuar vendas para clientes com capacidade para pagar	Perda parcial ou total devido a garantias insuficientes	
Produzir medicamentos conforme especificações técnicas	Insumos farmacêuticos fora do padrão	
Evitar perda de bens permanentes	Furto	
Zelar pela conduta ética dos funcionários	Conduta inadequada devido a desconhecimento por parte de funcionários	

Controles preventivos

- Concebidos para reduzir a frequência de materialização de eventos de risco. Atuam sobre a probabilidade de ocorrência de um determinado evento, dificultando seu acontecimento.
- Agem como guia, auxiliando para que fatos aconteçam de acordo com o previsto, procurando prevenir, de antemão, problemas ou desvios do padrão.
  - **Exemplos:** políticas, normas, manuais, unidade de auditoria ou de controle interno, processos de planejamento, de gestão de riscos, sistema de controle interno etc.

Controles detectivos

- Concebidos para detectar a materialização de eventos de risco; contudo não impedem a sua ocorrência.
- Alertam sobre a existência de problemas ou desvios do padrão, portanto exigem informação para comparação.
- Ações corretivas devem ser concebidas juntamente e para cada controle detectivo projetado.
  - **Exemplos:** conciliações, inventários, revisões independentes, monitoramento e análises críticas de indicadores etc.

Avaliação de um risco

- O risco inerente é o “risco bruto” e seu nível pode estar acima do apetite a risco da organização. Neste caso, controles são estabelecidos para reduzir o risco a um nível aceitável.

Risco Inerente – Efeito do Controle = Risco Residual

Avaliação de um risco

- A avaliação do risco se completa ao se considerar o efeito dos controles sobre os riscos inerentes.
- Em tese, quanto melhor o controle, menor será o risco residual.
- Para isso, os controles existentes para cada risco devem ser identificados e avaliados. A escala a seguir apresenta um método para avaliar a eficácia dos controles e estimar o nível dos riscos residuais em função dessa eficácia.

Escala para avaliação de Controles

Situação do controle existente	Avaliação	Multiplicador do Risco Inerente
Ausência completa de controle.	(1) Inexistente	1,00
Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	(2) Fraco	0,80
Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	(3) Mediano	0,60
Controle normatizado e embora passível de aperfeiçoamento, está sustentada por ferramentas adequadas e mitiga o risco razoavelmente.	(4) Satisfatório	0,40
Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrada num nível de “melhor prática”.	(5) Forte	0,20

Registro de Riscos

Função/ Atividade	Compilado por	Data
Objetivo	Analisado por	Data

Riscos Identificados			Avaliação			Controles Existentes		Risco Residual	Recomendação	
Eventos	Causas	Consequências	Prob.	Impacto	Nível	Descrição	Eficácia		Tratar risco	Prior.

Vamos trabalhar na Avaliação de riscos

- Em grupos de 3 a 4 pessoas, preencham no **Registro de Riscos** as colunas ‘Controles Existentes’ e ‘Risco Residual:

  - ✓Identifique os controles existentes e avalie a sua eficácia, levando em conta o seu desenho e implementação, indicando na coluna ‘Eficácia’, a ‘Avaliação’ do controle efetuada conforme a Escala para avaliação de controles apresentada.
  - ✓Na coluna ‘Risco Residual’, indique o resultado da multiplicação do Nível de risco inerente pelo número indicado na coluna ‘Multiplicador do Risco Inerente’ que corresponda à avaliação da eficácia do controle.

Sessão 0.2

Controle Interno e suas limitações

Os participantes deverão ser capazes, ao final da sessão, de conceituar processo de controle interno e reconhecer limitações que afetam sua eficácia.

- O processo de identificação e avaliação de riscos é essencial para se estabelecer controles apropriados que redundem em maior possibilidade de que os resultados organizacionais pretendidos sejam alcançados.

Definição de controle interno (COSO)

- **Controle interno** é um processo conduzido pela estrutura de governança e por gestores e profissionais da organização, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.
- **Controle** é uma política ou procedimento que faz parte do controle interno.

Compreendendo a definição do COSO

- Conduzido para atingir **objetivos** em uma ou mais categorias – operacional, divulgação e conformidade.
- Um **processo** que consiste em tarefas e atividades contínuas – um meio para um fim, não um fim em si mesmo.
- Realizado por **pessoas** – não se trata simplesmente de manuais de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da organização para realizar o controle interno.
- Capaz de proporcionar **segurança razoável** – porém não absoluta, para a alta administração de uma organização.
- **Adaptável** à estrutura da entidade – flexível na aplicação para toda a organização ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

Acepções de “Controle Interno”

- A expressão **controle interno** é utilizada para se referir ao **conjunto de políticas, procedimentos e atividades** que uma organização adota para gerenciar seus objetivos, mediante tratamento dos riscos a eles associados.
- No setor público, a expressão é também utilizada para **designar os órgãos e as unidades** responsáveis por avaliar aquele conjunto de políticas, procedimentos e atividades.
  - Administração direta: **Controle Interno**
  - Administração indireta: **Auditoria Interna**
  - Denominações da unidade responsável: secretaria, coordenação, unidade etc.

Limitações do controle interno

- O modelo COSO reconhece que, apesar de o controle interno fornecer razoável segurança quanto ao alcance dos objetivos da entidade, existem limitações.
- Controle interno não pode evitar julgamentos ou decisões ruins, ou ainda eventos externos que podem levar a organização a falhar na busca de seus objetivos.
- Mesmo um SCI efetivo pode vir a falhar.
- A administração deve estar **consciente dessas limitações** ao selecionar, desenvolver e implantar controles para buscar minimizá-las.

Limitações do controle interno

Limitações podem se originar, por exemplo, destes **fatores**:

- inadequação dos objetivos estabelecidos
- julgamento humano na tomada de decisão pode ser falho e sujeito a viés
  - Decisões precisam ser tomadas sob pressões de tempo e outras decorrentes da condução dos negócios, com base em informações disponíveis, o que afeta a qualidade da decisão
- capacidade da gerência para passar por cima do controle interno. Exemplos:
  - omissão de cotações mais vantajosas para favorecer determinados fornecedores
  - atestação de despesas não executadas ou superfaturadas

Limitações do controle interno

- capacidade de gestores, funcionários e/ou terceiros para contornar os controles por meio de conluio
  - Ações intencionais de gestores para obter benefícios para si ou para outrem, para evitar sanções, para maquiar resultados, entre outros motivos
  - Exemplo: elaboração de pareceres insubsistentes para aprovação de aplicação de recursos
- falha humana, mesmo com controles bem desenhados:
  - Pessoas podem não entender instruções ou interpretá-las de forma equivocada.
  - Podem, ainda, cometer erros por fadiga, distração ou falta de cuidado (erros de execução)

Limitações do controle interno

- controles podem conter erros de desenho, o que leva a perpetuação das falhas (erros de procedimento)
- eventos externos que escapam ao controle da organização

Custo x benefício de um controle

- Dadas as limitações de recursos em qualquer organização, controles devem ser adotados considerando-se os custos envolvidos, que não devem ser superiores às perdas decorrentes da consumação do risco que se pretende com ele controlar.
- Procedimentos ou atividades de controle devem ser **seletivos**, eliminando-se aqueles em que o risco é avaliado como baixo.
- Em certas circunstâncias, mesmo sendo o risco elevado, o custo do controlá-lo é inviável.

Evolução da atuação da Auditoria Interna