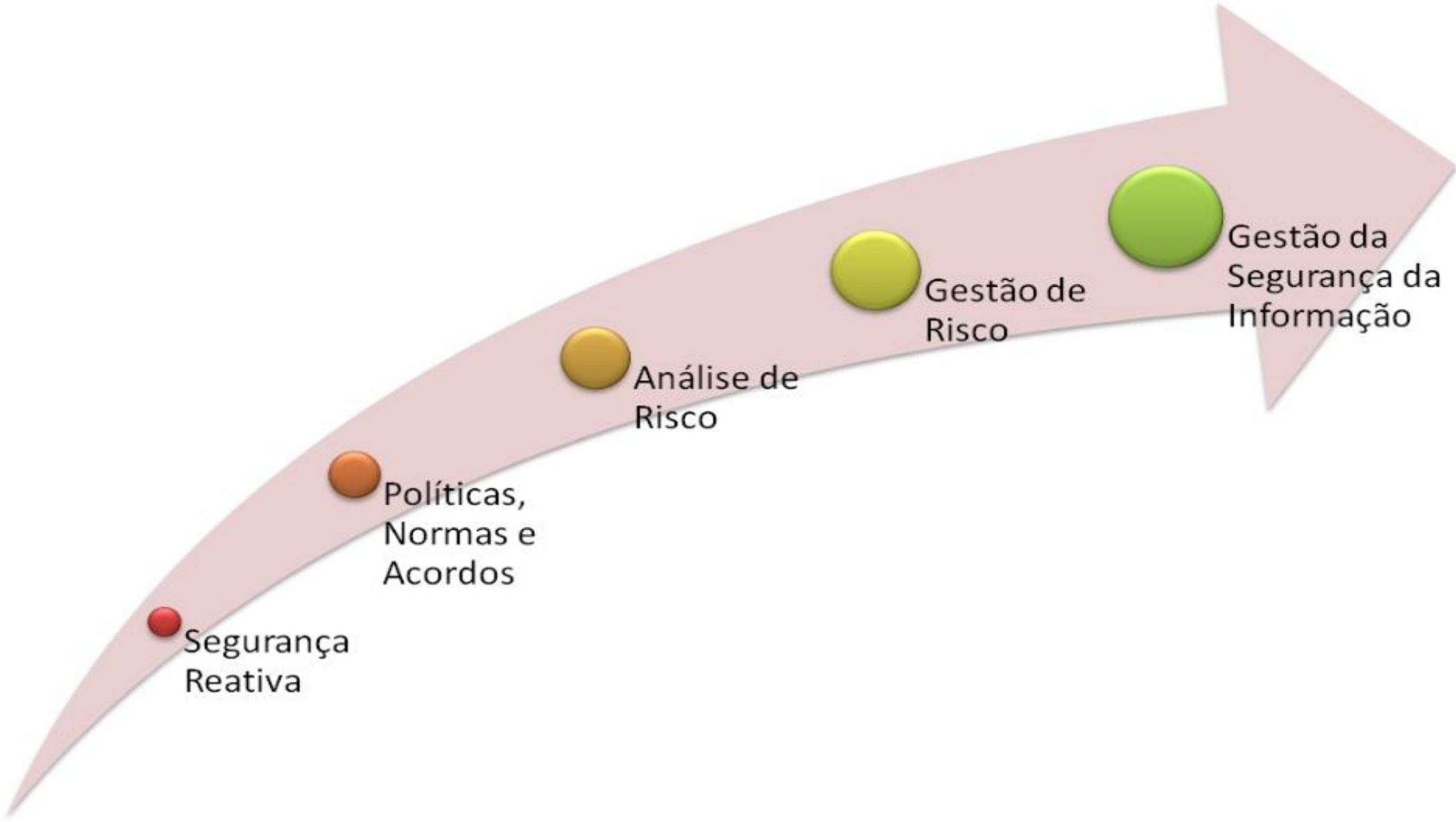
Gestão de Risco



Gestão de Risco

- Unidade 2 -Gestão de Risco
- 2.1- O que é gestão de risco
- 2.2- Processo de gestão de risco
- 2.2.1- Análise e avaliação de riscos
- 2.2.2- Tratamento dos riscos
- 2.2.3- Aceitação dos riscos
- 2.2.4- Comunicação dos riscos
- 2.2.5- Monitoramento dos riscos


Riscos Residuais
Riscos Secundários
Identificação
Identificar os riscos e compreender algumas de suas características para análise posterior
1
2
Análise Qualitativa
Compreender a importância do risco através de escalas médias de impacto e probabilidade
3
Análise Quantitativa
Investigar o impacto e efeitos do risco com precisão numérica
4
Planejamento de Respostas
Decidir como lidar com cada risco considerando a tolerância ou aversão a riscos predominante
5
Monitoramento
Acompanhar o comportamento dos riscos no tempo e a adequação do nível de exposição existente
Gerenciamento de Riscos

Conceitos de Risco

- Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;
- Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;
- Gestão de riscos: arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;
- Gerenciamento de risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais.

O que é Gestão de Risco

- Risco pode ser bom. Sem risco não haveria recompensa.
- O objetivo de gerenciar riscos não é eliminá-los, mas entendê-los de forma a ter benefícios com os aspectos positivos e minimizar os aspectos negativos.
- Isto requer clareza sobre quais riscos você está preparado para enfrentar, o quanto está preparado e se você tem processos para gerenciar estes riscos.
- **O principal objetivo da Gestão de Riscos é avaliar as incertezas do Projeto.**

O que é Gestão de Risco

- Gestão de riscos é o processo de organizar e planejar recursos humanos e materiais de uma empresa de forma a reduzir ao mínimo possível os impactos dos riscos na organização, utilizando um conjunto de técnicas que visa minimizar os efeitos dos danos acidentais direcionando o tratamento aos riscos que possam causar danos ao projeto, às pessoas, ao meio ambiente e a imagem da empresa.

O que é Gestão de Risco

- O principal objetivo da Gestão de Riscos é avaliar as incertezas de forma a tomar a melhor decisão possível. De certa forma, toda gestão de risco e toda tomada de decisão lida com esta situação, e os seus benefícios dão as melhores decisões, menos surpresa, melhora no planejamento, na performance e na efetividade, além da melhora no relacionamento com as partes interessadas.

O que é Gestão de Risco

Segundo o Guia PMBOK quinta edição, os processos de gerenciamento de riscos do projeto incluem os seguintes pontos:

- **Planejar o gerenciamento dos riscos:** processo de definição de como conduzir as atividades de gerenciamento dos risco de um projeto;
- **Identificar os Riscos:** processo de determinação dos riscos que podem afetar o projeto e de documentação de suas características;
- **Realizar a Análise Qualitativa dos Riscos**: processo de priorização dos riscos para análise ou adicional através da avaliação e combinação de sua probabilidade de ocorrência e impacto;
- **Realizar a Análise Quantitativa dos Riscos:** processo de analisar numericamente o efeito dos riscos identificados, nos objetivos gerais do projeto;
- **Planejar as Respostas aos Riscos:** processo de desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças ao projeto;
- **Monitorar e Controlar os Riscos:** processo de implementação dos planos de respostas aos riscos, acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação de novos riscos e avaliação da eficácia dos processos de tratamento dos riscos durante todo o projeto.

O que é Gestão de Risco

No COBIT 4.1 é recomendado que os riscos devem ser gerenciados das seguintes formas:

- **Mitigação de Riscos:** implementação de controles que protejam contra riscos, como por exemplo, implementação de um firewall de segurança;
- **Transferência de Riscos:** compartilhar riscos com parceiros ou contratar seguro apropriado;
- **Aceitação de Riscos:** confirmação e monitoração de riscos, e ter um plano de resposta ao risco pronto;
- **Evitar Riscos:** adotar uma opção diferente que evite completamente o risco.

COBIT é a sigla para “Control Objectives for Information and related Technology” e que, na prática, significa uma estrutura capaz de fornecer governança de TI.

Processo de Gestão de Risco

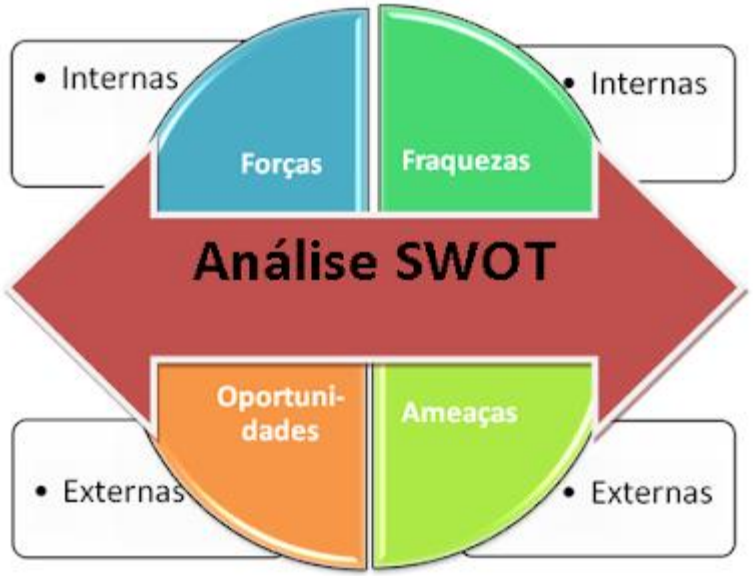
- Riscos são importantes para as decisões estratégicas, são também a principal causa das incertezas nas organizações e estão presentes nas atividades mais simples de uma empresa.
- Uma abordagem ampla e corporativa da gestão de riscos permite que uma organização contabilize o potencial impacto de todos os tipos de riscos em todos os seus processos, atividades, produtos e serviços.

Processo de Gestão de Risco

- A premissa inerente à gestão de riscos corporativos (ERM – *Enterprise Risk Management*) é que toda organização existe para gerar valor às partes interessadas.
- Todas as organizações enfrentam incertezas e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza e definir como ela pode interferir no esforço para gerar valor às partes interessadas.

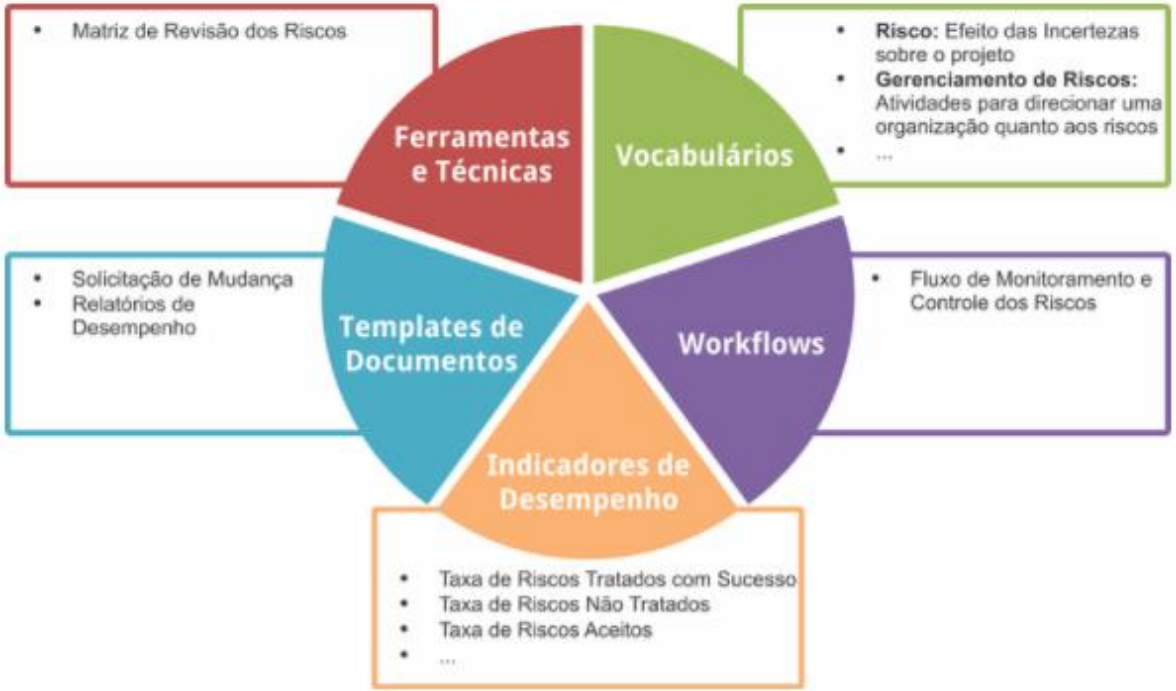
Processo de Gestão de Risco

- Incertezas representam riscos e oportunidades que têm potencial para destruir ou agregar valor.
- A gestão de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.



Processo de Gestão de Risco

- Uma iniciativa bem-sucedida de gestão de riscos corporativos pode afetar a probabilidade e o impacto de possíveis riscos, assim como proporcionar benefícios relacionados a decisões estratégicas mais bem fundamentadas, processos de mudança bem-sucedidos e aumento da eficiência operacional.



Processo de Gestão de Risco

- Outros benefícios incluem a redução do custo do capital, relatórios financeiros mais precisos, vantagem competitiva, melhoria da percepção da organização, melhor presença de mercado e, no caso de organizações de serviço público, aprimoramento no apoio político e comunitário.

Processo de Gestão de Risco

- Em um processo de gestão de riscos podem existir várias etapas e atividades. Mas o ciclo de vida completo da gestão de riscos pode ser resumido em apenas 5 delas, que são a base para os principais regulamentos de gestão de riscos, incluindo o COSO e a ISO 31000.
  - O **COSO®** (***Committee of Sponsoring Organizations of the Treadway Commission***) é uma organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nos procedimentos e processos internos da empresa.
  - ISO 31000 é uma norma da família de gestão de risco criada pela International Organization for Standardization. O objetivo da ISO 31000: 2009 é estabelecer princípios e orientações genéricas sobre gestão de riscos.
- São elas:

Processo de Gestão de Risco

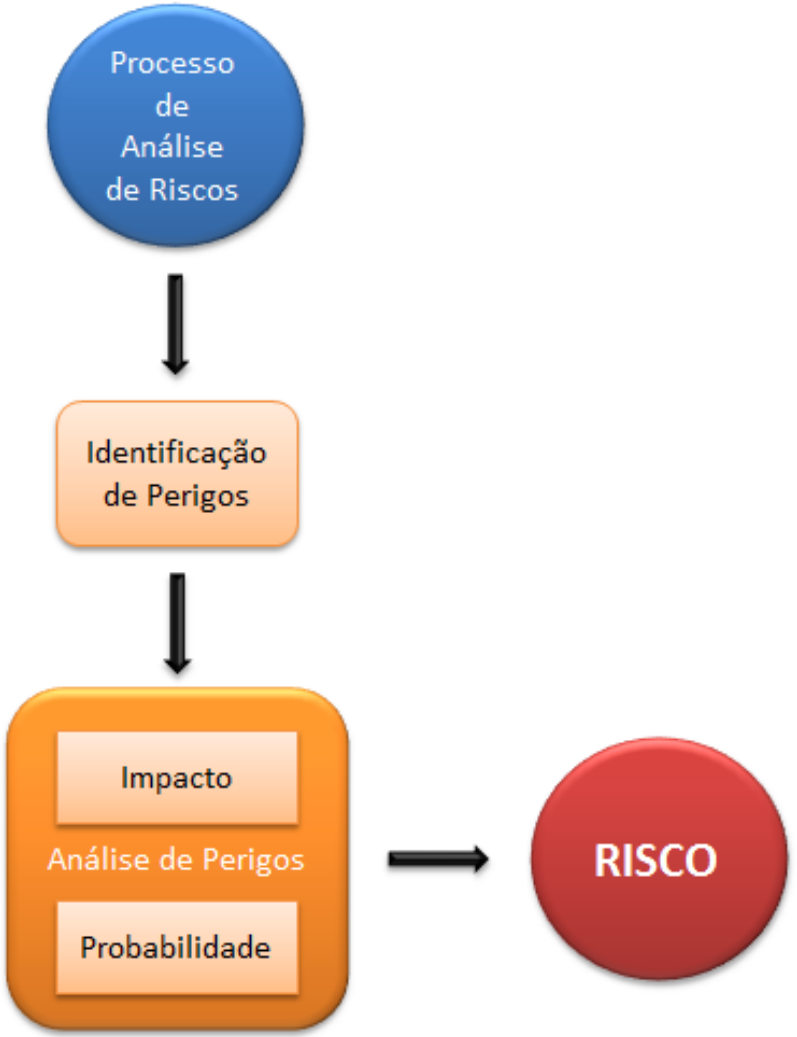
1. Identificação

- O ponto de partida é descobrir os riscos e defini-los com algum detalhamento e em um formato estruturado.

Processo de Gestão de Risco

2. Avaliação

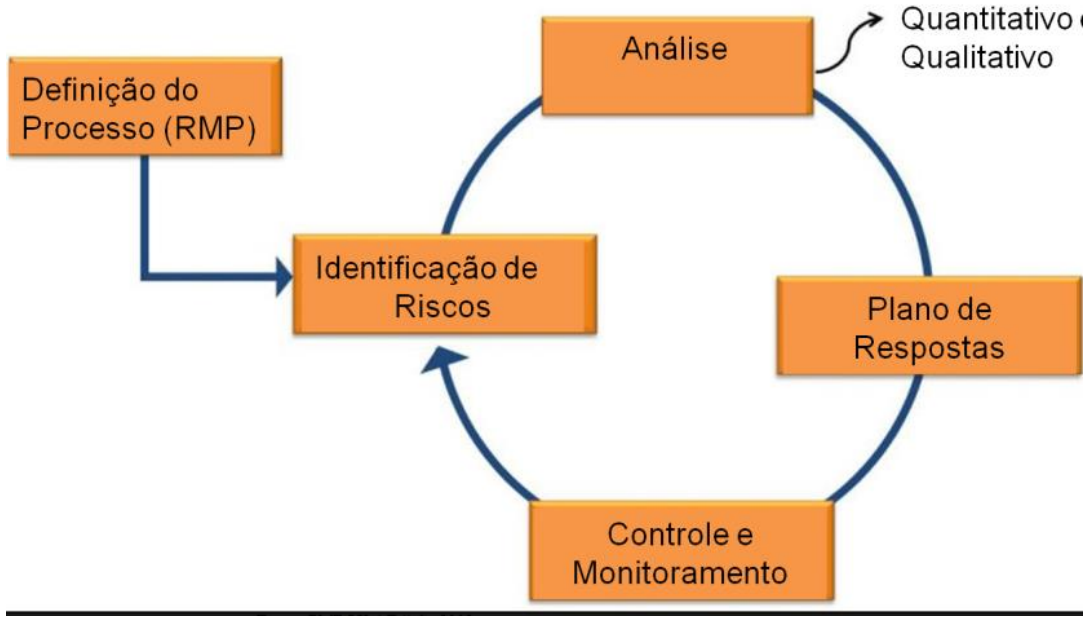
- Os riscos são avaliados quanto a probabilidade e o impacto de sua ocorrência.



Processo de Gestão de Risco

3. Tratamento

- Uma abordagem para o tratamento de cada risco deve ser definida, que em alguns casos pode ser não fazer nada. Isso requer uma análise da aceitabilidade do risco, podendo requerer um plano de ação para prevenir, reduzir ou transferir o risco.



Processo de Gestão de Risco

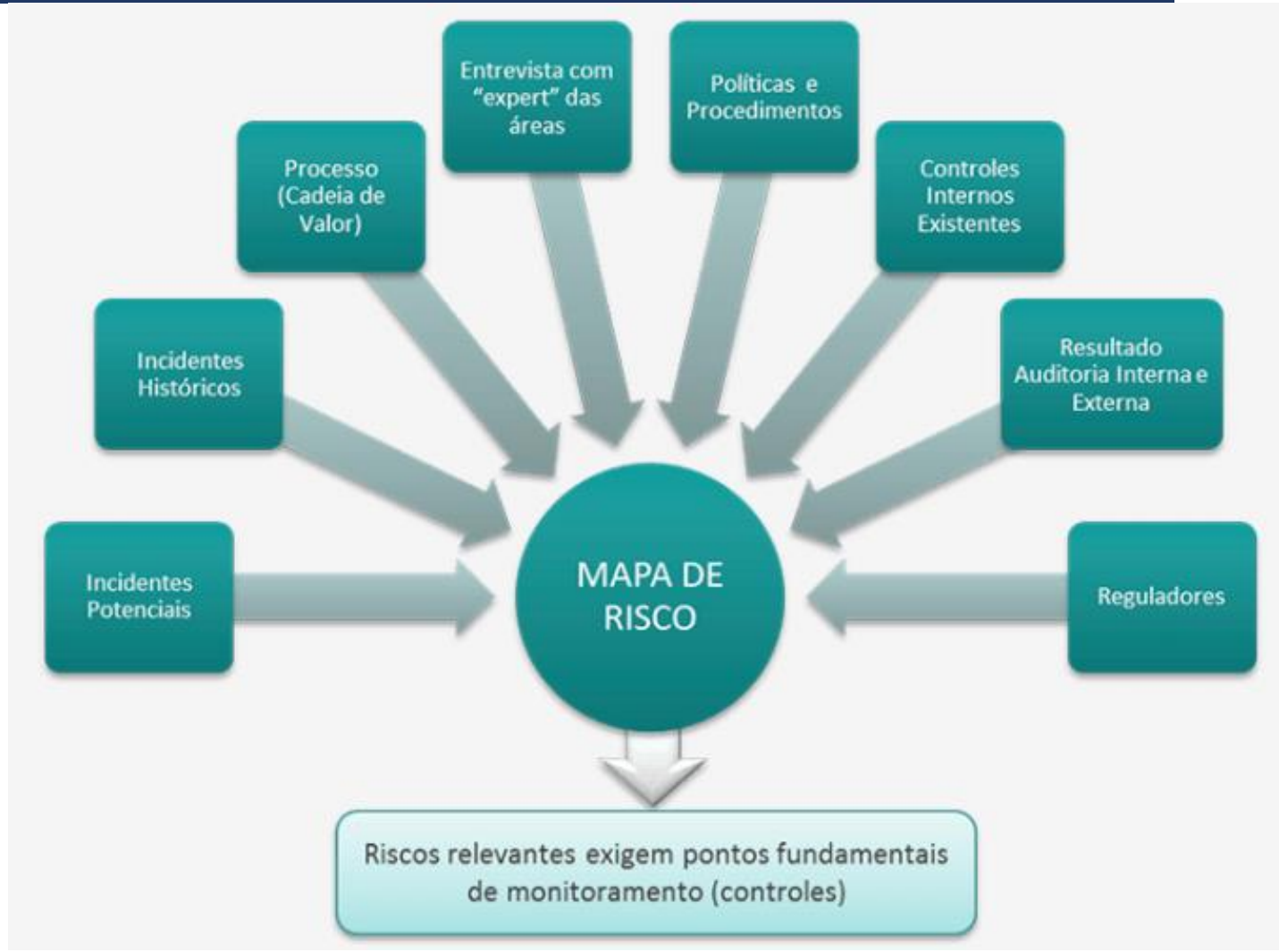
4. Monitoramento

- Um processo contínuo de revisão é essencial para uma gestão de riscos proativa, reavaliando os riscos e monitorando a situação dos tratamentos e controles implementados.

Processo de Gestão de Risco

5. Comunicação

- A comunicação em cada uma destas quatro etapas anteriores é parte fundamental para um processo de tomada de decisão efetivo na gestão de riscos.



Análise e Avaliação de Riscos

- Definir risco é bastante complexo, existindo alguns que dizem que ele é o grau de incerteza em relação à possibilidade de ocorrência de um determinado evento, o que, se realizado, redunda em prejuízos, ou seja, risco é a possibilidade de perda decorrente de um determinado evento.
- Nesse caso, perda para a empresa significa prejuízo, lucro menor, ou redução de ativos com contrapartida no patrimônio líquido.

Análise e Avaliação de Riscos

- Outros afirmam que os riscos empresariais são todos os eventos que impedem a empresa e as pessoas de ganharem dinheiro e respeito.
- São elementos incertos e as expectativas que agem constantemente sobre os meios estratégicos e o ambiente e que provocam os desastres financeiros.

Análise e Avaliação de Riscos

A gestão de riscos inclui:

- A aplicação de métodos lógicos e sistemáticos para a comunicação e consulta ao longo de todo processo;
- O estabelecimento do contexto para identificar, analisar, avaliar e tratar o risco associado a qualquer atividade, processo, função ou produto;
- O monitoramento e a análise crítica de riscos;
- O reporte e o registro dos resultados de forma apropriada;
- O processo de avaliação de riscos é a parte da gestão de riscos que fornece um processo estruturado para identificar como os objetivos podem ser afetados, e analisa o risco em termos de consequências e suas probabilidades antes de decidir se um tratamento adicional é requerido.

Análise e Avaliação de Riscos

O processo de avaliação de riscos tenta responder às seguintes questões fundamentais:

- O que pode acontecer e por quê (pela identificação de riscos)?;
- Quais são as consequências?
- Qual é a probabilidade de sua ocorrência futura?
- Existem fatores que mitigam a consequência do risco ou que reduzam a probabilidade do risco?
- O nível de risco é tolerável ou aceitável e requer tratamento adicional?

Análise e Avaliação de Riscos

Eventos já ocorridos que tenham sido investigados, com causas identificadas e medidas de prevenção de recorrência adotadas, é de pressupor que não ocorrerá mais.

Análise e Avaliação de Riscos

- A NBR ISO/IEC 31010:2012 é uma norma de apoio à NBR ISO 31000 e fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.
- O processo de avaliação de riscos conduzido de acordo com essa norma contribui para outras atividades de gestão de riscos.

Análise e Avaliação de Riscos

- O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.
- Os riscos podem ser avaliados em nível organizacional, em nível departamental, para projetos, atividades individuais ou riscos específicos.
- O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades.

Análise e Avaliação de Riscos

Isso proporciona uma entrada para decisões sobre:

- Se convém que uma atividade seja realizada;
- Como maximizar as oportunidades;
- Se os riscos necessitam ser tratados;
- A escolha entre opções com diferentes riscos;
- A priorização das opções de tratamento de riscos.

Análise e Avaliação de Riscos

- A seleção mais apropriada de estratégias é o tratamento de riscos que trará riscos adversos a um nível tolerável.
- Completado um processo de avaliação de riscos, o tratamento de riscos envolve selecionar e acordar uma ou mais opções pertinentes para alterar a probabilidade de ocorrência, o efeito dos riscos, ou ambos, e a implementação destas opções.
- Isso é acompanhado por um processo cíclico de reavaliação do novo nível de risco, tendo em vista a determinação de sua tolerabilidade em relação aos critérios previamente definidos, a fim de decidir se tratamento adicional é requerido.

Tratamento dos Riscos

Uma vez que você tenha uma lista de riscos inaceitáveis, você tem que ir de um por um e decidir como trata-los – geralmente, estas opções são aplicadas:

- **Diminuir o risco** – esta opção é a mais comum, e ela inclui a implementação de salvaguardas (controles) – como sistemas de supressão de incêndio, etc.
- **Evitar o risco** – parar de realizar certas tarefas ou processos se eles incorrem em riscos que são simplesmente muito grandes para mitigar com quaisquer outras opções – e.g., você pode decidir banir o uso de laptops fora das instalações da empresa se o risco de acesso não autorizado para estes laptops é muito alto (porque, e.g., tais comprometimentos poderiam paralisar completamente a infraestrutura de TI que você está usando).
- **Compartilhar o risco** – isto significa você transferir o risco para outra parte – e.g., você compra uma apólice de seguro para o seu prédio contra incêndio, e assim você transfere parte do seu risco financeiro para uma companhia de seguro. Infelizmente, esta opção não tem qualquer influência no incidente em si, então a melhor estratégia é usar esta opção em conjunto com opções 1) e 2).
- **Reter o risco** – esta é a opção menos desejada, e significa que sua organização aceita o risco sem fazer nada a respeito. Esta opção deveria ser usada apenas se os custos de mitigação forem maiores do que o dano que um incidente poderia causar.

Tratamento dos Riscos

Antes de você iniciar o tratamento de riscos

- Antes de iniciar o processo de Tratamento de risco, deve-se estar ciente das principais entradas: estas são a Metodologia de Gestão de Riscos e riscos inaceitáveis da avaliação de riscos; contudo, uma entrada adicional também deveria ser o orçamento disponível para o ano corrente, porque muito frequentemente a mitigação irá requerer um investimento.

A palavra **mitigar** significa atenuar, abrandar. Já a palavra **risco** está atrelada à incerteza de que algo aconteça. Quando falamos em **mitigação de riscos** operacionais, estamos nos referindo, portanto, à atenuação dos impactos que uma falha processual pode trazer para a empresa.

Tratamento dos Riscos

Quando da seleção de novos controles, basicamente existem três tipos de controles:

- **Definir novas regras:** regras são documentadas através de planos, políticas, procedimentos, instruções, etc., embora você não tenha que documentar alguns processos menos complexos.
- **Implementar novas tecnologias:** por exemplo, sistemas de backup, locais de recuperação de desastre para data centers alternativos, etc.
- **Mudar a estrutura organizacional:** em alguns casos, você precisará introduzir uma nova função de trabalho, ou mudar as responsabilidades de uma posição existente.

Tratamento dos Riscos

- O processo de tratamento de riscos é muito frequentemente documentado de forma similar ao processo de avaliação de riscos – através de planilhas Excel ou uma ferramenta, e finalmente, no Relatório de Tratamento de Riscos. Um exemplo de uma tabela de tratamento de riscos pode se parecer como algo a seguir:

Tratamento dos Riscos

Ativo	Ameaça	Vulnerabilidade	Opção de tratamento	Meios de implementação
Servidor	Incêndio	Ausência de extintor de incêndio	1) Diminuir o risco + 2) Compartilhar o risco	Comprar extintor de incêndio + comprar apólice de seguro contra incêndio
Laptop	Acesso por pessoas não autorizadas	Senha inadequada	1) Diminuir o risco	Elaborar Política de Senha
Administrador de sistema	Deixar a organização	Sem substituto	1) Diminuir o risco	Contratar segundo administrador de sistema que aprenderá tudo que o primeiro faz

Aceitação dos Riscos

- Uma técnica de planejamento de respostas a riscos que indica que a equipe do projeto decidiu não alterar o plano de gerenciamento do projeto para lidar com um risco ou que não consegue identificar uma outra estratégia de resposta adequada.

Aceitação dos Riscos

- Possibilitar o desenvolvimento de estratégias de tratamento de elaboração de planos emergenciais aos riscos somente à medida que surgem. Historicamente sempre ocorrem, em grau maior ou menor.
- Quando aceite-se riscos sempre existe um preço a ser pago (prazo, custo, etc..) por esta aceitação. O desenvolvimento de um plano prévio pode diminuir diversas dores de cabeça nessa hora.
- De maneira geral, aceitar riscos é admitir a possibilidade da ocorrência ou não do imprevisível.

Aceitação dos Riscos

- Mitigação de Riscos: Nos projetos de software a estratégia de mitigação tem se evidenciado como uma prática bem adequada, porque pode contar com um universo de modelos (templates), resultado de lições aprendidas(desenvolvidas) em projetos símiles.
- Esta estratégia orienta que se deve mensurar as probabilidades da ocorrência dos eventuais riscos e a redução das consequências adversas.
- Para tanto é importante que o Gerente de Projetos possa identificar os riscos associados aos projetos desde a sua fase inicial.

Comunicação dos Riscos

- Comunicação de Risco pode ser entendida como um processo de Comunicação que auxilia os gestores em suas decisões em relação aos seus Stakeholders – públicos de interesse.
- Além disso, tal estratégia é responsável por gerar um maior entendimento sobre o grau e a natureza dos perigos que ameaçam a organização.

Comunicação dos Riscos

- A comunicação de risco é um tema complexo e abrangente ao envolver situações de risco, sejam eles decorrentes de ações humanas, naturais ou industriais.

Comunicação dos Riscos

- O princípio da comunicação de risco é importante instrumento a ser incorporado à gestão organizacional a fim de melhorar a capacidade de diálogo das organizações com suas partes interessadas, de modo a tornar possível a incorporação desses princípios ao processo de tomada de decisão sobre como os riscos devem ser gerenciados.

Comunicação dos Riscos

- Ao se incorporar tais princípios no processo de tomada de decisão, contribui-se para que diferentes partes interessadas desenvolvam correta percepção a respeito da dimensão dos riscos existentes para, dessa forma, buscarem consenso a fim de compatibilizar interesses aparentemente divergentes.

Comunicação dos Riscos

- De acordo com Renn (2006), gerenciamento de risco é um procedimento lógico e interativo mantido pela adoção sistemática de políticas, procedimentos e práticas organizacionais com o objetivo de estabelecer os contextos dos riscos, identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos associados.
- O processo de gerenciamento de riscos gera informações que permitem ao tomador de decisão melhor compreender os riscos existentes e seus possíveis impactos, possibilitando às organizações alternativas para minimizar perdas e identificar oportunidades.

Monitoramento de Riscos

- O processo de implementação de planos de respostas aos riscos, acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação de novos riscos e avaliação da eficácia dos processos de tratamento dos riscos durante todo o projeto.

Monitoramento de Riscos

- As respostas planejadas aos riscos que são incluídas no plano de gerenciamento do projeto são executadas durante todo o ciclo de vida do projeto, mas o trabalho do projeto deve ser continuamente monitorado em busca de riscos novos, modificados e desatualizados.

Monitoramento de Riscos

- O processo de monitorar e controlar os riscos utiliza técnicas, como análises de variações e tendências, que requerem o uso das informações de desempenho geradas durante a execução do projeto.
- Todas as fases de um projeto envolvem riscos. A todo momento em que se planeja, também se sabe que o resultado pode ocorrer de maneira diferente da esperada. A dicotomia estabelecida entre risco e retorno faz-se presente em todas as esferas do ambiente de um projeto, não ficando restrito somente ao campo financeiro.

Monitoramento de Riscos

- Outras finalidades do processo de monitorar e controlar os riscos determinam se:
  - As premissas do projeto ainda são válidas;
  - A análise mostra um risco avaliado que foi modificado ou que pode ser desativado;
  - As políticas e os procedimentos de gerenciamento dos riscos estão sendo seguidos;
  - As reservas para contingências de custo ou cronograma devem ser modificadas de acordo com a avaliação atual dos riscos.

Monitoramento de Riscos

ENTRADAS	FERRAMENTAS E TÉCNICAS	SAÍDAS
1. Registro dos riscos	1. Reavaliação de riscos	1. Atualizações do registro dos riscos
2. Plano de gerenciamento do projeto	2. Auditorias dos riscos	2. Atualizações dos Ativos de processos organizacionais
3. Informações sobre desempenho do trabalho	3. Análises de variação e tendências	3. Solicitações de mudança
4. Relatórios de desempenho	4. Medição de desempenho técnico	4. Atualizações do plano de gerenciamento do projeto
	5. Análise de reservas	5. Atualizações dos documentos do projeto
	6. Reuniões de andamento	

Perigo

Risco

Atividade Avaliativa – Análise de SWOT

- Análise de Swot
- SWOT é a sigla dos termos ingleses ***Strengths*** (Forças), ***Weaknesses*** (Fraquezas), ***Opportunities*** (Oportunidades) e ***Threats*** (Ameaças) que consiste em uma **ferramenta de análise** bastante popular no âmbito empresarial.
- Consiste em recolher dados importantes que caracterizam o **ambiente interno** (forças e fraquezas) e **externo** (oportunidades e ameaças) da empresa.

Atividade Avaliativa – Análise de SWOT

Atividade Avaliativa – Análise de SWOT

Atividade Avaliativa – Análise de SWOT

- *Strengths* (**forças**) - vantagens internas da empresa em relação às concorrentes. Ex.: qualidade do produto oferecido, bom serviço prestado ao cliente, solidez financeira, etc.
- *Weaknesses* (**fraquezas**) - desvantagens internas da empresa em relação às concorrentes. Ex.: altos custos de produção, má imagem, instalações desadequadas, marca fraca, etc.;
- *Opportunities* (**oportunidades**) – aspectos externos positivos que podem potenciar a vantagem competitiva da empresa. Ex.: mudanças nos gostos dos clientes, falência de empresa concorrente, etc.;
- *Threats* (**ameaças**) - aspectos externos negativos que podem por em risco a vantagem competitiva da empresa. Ex.: novos competidores, perda de trabalhadores fundamentais, etc.

Atividade Avaliativa – Análise de SWOT

Análise Swot Cruzada

- A análise swot cruzada consiste em cruzar as informações dos quatro quadrantes, de forma a obter um moldura que permita delinear estratégias importantes para o futuro da empresa/instituição.
- Para a análise SWOT Cruzada é preciso primeiro fazer uma análise clara do ambiente, ou seja, pesquisar profundamente as forças e fraquezas e saber identificar as oportunidades e ameaças. Para cada cruzamento é importante saber criar objetivos/estratégias:
- Pontos fortes x Oportunidades = estratégia ofensiva / desenvolvimento das vantagens competitivas.
- Pontos fortes x Ameaças = estratégia de confronto para modificação do ambiente a favor da empresa.
- Pontos fracos x Oportunidades = estratégia de reforço para poder aproveitar melhor as oportunidades.
- Pontos fracos x Ameaças = estratégia defensiva com possíveis modificações profundas para proteger a empresa.

Atividade Avaliativa – Análise de SWOT

Complemente a Análise de SWOT já criada relacionada à Estruturação da Área de TI.

FORÇAS	FRAQUEZAS	OPORTUNIDADES	AMEAÇAS
Maioria dos Servidores em Cloud	Falta de Treinamento de Serviços na Nuvem	Uso de Softwares Livres	Corte de Orçamentos
Service Desk em Cloud	Atendimento de Chamados demorado	Melhor Uso dos Equipamentos e Sistemas	Obsolescência dos Equipamentos de Impressão
Célula de Desenvolvimento de Sistemas Interno	Falta de Integração entre as Áreas	Armazenagem em Nuvem	Aumento de Compartilhamento de Arquivos e Risco de Vírus
Banco de Dados Oracle	Dificuldade em atender necessidades de Negócio dos Usuários	Compartilhamento de Documentos na Nuvem	Crescimento dos Crimes Cibernéticos
Telefonia Fixa IP	Falta de Redundância da Rede	Uso de Novas Tecnologias	Falta de Suporte de Fabricantes
Todas as Máquinas com Windows 10	Falta de Planos de Disaster Recovery	Tecnologia das Coisas (IoT)	Não ter Governança de TI
Usam Office 365	Falata de Plano de Gestão de Riscos	Treinamento sobre Segurança da Informação	Não Invetimento em Treinamentos Técnicos