AULA 05: Governança de TI: Noções de Cobit e Riscos em TI.

SUMÁRIO	PÁGINA

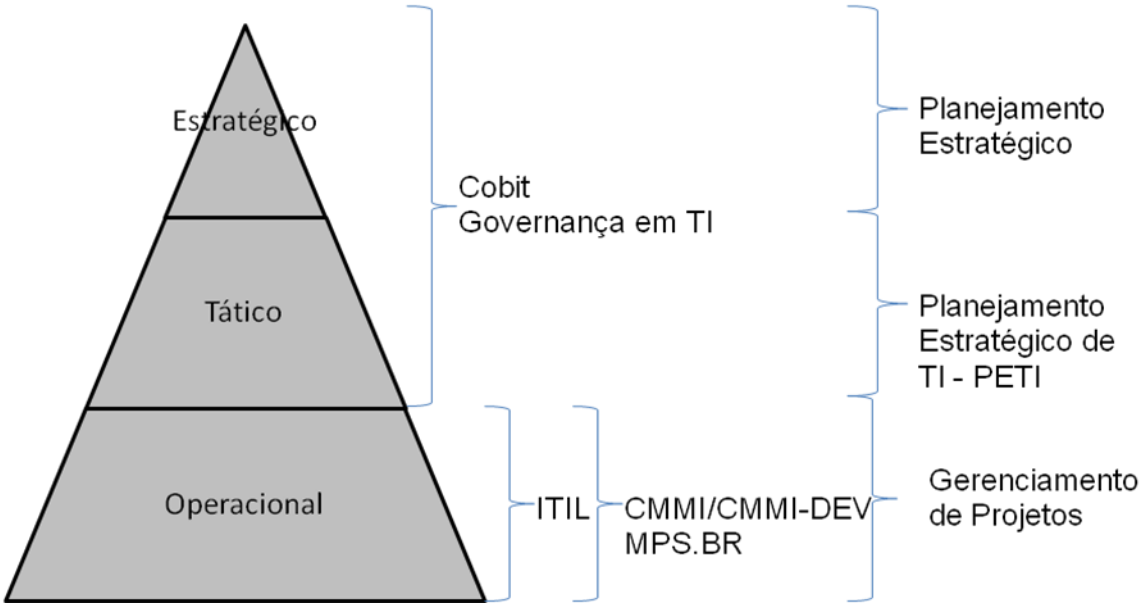
Olá Concurseiros de Plantão!

Vamos falar um pouco sobre Governança de TI, Cobit 4.1 e Risco em TI, trataremos claro somente de tópicos que vem sendo cobrados em concursos públicos da melhor forma possível para que possam gabaritar todas as questões que venham a cair na tua prova sobre o assunto.

Seguiremos a seguinte estrutura de apresentação do conteúdo:

- Conceitos Básicos / Modelo Cobit.
- Planejar e Organizar.
- Adquirir e Implementar.
- Entregar e Suportar.
- Monitorar a Avaliar.
- Riscos em Tecnologia da Informação.

1 Conceitos Básicos.



Claro que não poderia deixar de ser né concurseiros, trago-lhes então uma das melhores visões didáticas que temos quando falamos em Gestão e Governança de TI, que é justamente o posicionamento no qual se encontra o Cobit em sua organização também como disciplina em suas

provas de concurso público, veja que ele está nos níveis tático e estratégico e não é atoa, pois quando falamos em Cobit nós estamos falando de Governança de TI e veremos no decorrer da nossa aula que a Governança de TI deverá ser garantida pela alta direção da nossa organização, ou seja, não é de responsabilidade do nível operacional.

1.1 Um pouco de história.

Para entendermos algumas das nossas disciplinas da área de TI, principalmente às que estão relacionadas à Gestão e Governança de TI, eu sempre gosto de trabalhar o assunto em características históricas e de evolução do conhecimento dos senhores, assim fica mais fácil de entender a origem, a necessidade do assunto que estamos tratando e também o motivo de sua formatação como está nos dias atuais.

Entre os anos 50 e 80 tivemos a era dos CPDs, para lembrá-los então foi a época na qual a informática começou a ganhar nome, pois neste momento o ser humano era capaz de registrar cálculos de balística em computadores e só esperar o resultado sair. Vemos que até então sabiam que existia algo acontecendo nas grandes organizações públicas e privadas, mas não sabiam afinal de contas o que realmente estava acontecendo, ou seja, os problemas eram resolvidos com informática, mas não se sabia como.

Nos anos 80 a 90 veio a era da Informação, época na qual tínhamos os computadores capacitados a realizar operações até então realizadas pelo ser humano e se tornando assim um grande motivador de demissões em massa que ocorreram nesta época, pois não que um computador tivesse tal capacidade de demissão em massa, mas que ele simplesmente assumia o papel de várias pessoas principalmente em operações corriqueiras e operacionais sobrevivendo assim somente aqueles que se prepararam e foram educados para trabalhar com a nova realidade.

Na década de 90 e 1ª metade do século XXI os computadores começaram a ser interconectados em uma grande rede chamada de Internet com

recursos de compartilhamento nunca visto antes e uma capacidade e publicação de conteúdo que não se podia ter em papel impressos nesta época.

Finalmente surge então a época da computação em nuvens, ou *Cloud Computing*, momento no qual o usuário tem a capacidade de além de armazenamento de todo o seu conteúdo na internet, também pode operacionalizar seu conteúdo e suas aplicações contando somente com os recursos que a internet lhe oferece, deste a leitura e resposta de e-mails até a edição e criação de poderosas planilhas eletrônicas e administração de bancos de dados.

Mas e então o que tal história tem a ver com o nosso assunto? Reparem então que com o passar dos anos o nível de complexidade no uso da Tecnologia da Informação aumentou em progressão geométrica quando comparado em razão da sua utilização e capacidade, isso tanto para os usuários domésticos quanto para as organizações (sejam elas da iniciativa pública ou privada) o que criou então uma grande necessidade de padronização de como Tecnologia da Informação – TI (chamaremos assim de agora em diante) deveria ser gerenciada ocasionando assim a criação de vários *frameworks* como podemos ver atualmente o ITIL, o Pmbok®, o CMMI.

Tal necessidade de atendimento ao nível de complexidade da TI nas instituições motivou também a evolução das contratações de bens de TI e aumentou a busca pela qualidade e alinhamento do que a TI realmente traria para a Administração Pública e como isso deveria ser pago, se era realmente necessário e justo para a Administração e se os resultados esperados seriam alcançados. (PPA, LDO, LOA).

Bem, não é para assustá-los, mas já conseguem reparar claramente que quando falamos em Cobit também falamos em vários outros assuntos, claro

que não com o nível de complexidade que trataríamos deles quando em um material exclusivo, mas precisamos tratar deles nem que em citações para fazermos as devidas ligações entre tais tópicos e a Governança de TI.

Neste momento então podemos ver claramente que a TI evoluiu caracterizada em alguns estágios bem identificados:

- TI como provedor de Tecnologia: momento no qual a TI fornecia respostas somente tecnológicas, algo como um apoio às necessidades que se tinham dela.
- TI como provedor de Serviços: momento no qual a TI iniciou sua trajetória no fornecimento de serviços de forma a agregar valor ao cliente.
- TI como parceiro estratégico: quando ela começou a ser valorizada dentro das instituições como um ativo estratégico.
- Tecnologia dos negócios: momento no qual podemos ver atualmente a TI como uma função principal dentro das organizações, a qual consegue se colocar em um patamar que a traz a visão de que se ela não existir na instituição, esta não irá sobreviver.

Tal evolução é claro que trouxe várias vantagens para as organizações, mas é claro que criou uma dependência considerável da TI para seu funcionamento, tanto que em alguns estudos realizados pela ITGI foi identificado que mais de 50% das empresas consideram a TI importante para a realização da sua estratégia, ou seja, atualmente a TI se tornou estratégica e crítica para as organizações o que gerou um aumento demasiado do impacto sob a instituição caso riscos da TI ocorram.

"Uma governança de TI efetiva ajuda a garantir que a TI suporte os objetivos de negócios, otimiza os investimentos em TI e apropriadamente os riscos e as oportunidades relacionados a TI." (ITGI).

1.2 O que é a Governança de TI então?

Vamos a algumas definições interessantes encontradas na literatura relacionada ao assunto que nos traz a idealização do que é Governança de TI.

"A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização." (ITGI).

"A governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios. A governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando em poder competitivo." (ITGI)

"Capacidade organizacional exercida pela alta direção, gerência de negócios e gerência de TI para controlar a formulação e implementação da estratégia de TI e, com isso, assegurar o alinhamento entre negócios e TI" (Van Grembergen, 2004)

Ficam claras então algumas características sobre o que vem a ser Governança de TI:

- É de responsabilidade da alta direção e gestão da organização.
- Trata-se de uma capacidade organizacional.
- De assegurar o alinhamento entre negócios e TI.

E então, já está com sono? Agüenta ai que o nosso conteúdo ainda está no começo.

Ficou claro então o que é Governança de TI? Ótimo, pois não podemos de forma alguma confundir Governança de TI com Gestão de TI

Gestão de TI ≠ Governança de TI, pois de uma forma geral a primeira está mais para as ferramentas utilizadas e a segunda mais para a capacidade organizacional.

1.3 Como a TI atende ao negócio?

Podemos reparar então que na atualidade executivos precisam de objetivos de controle. As organizações precisam de medidas objetivas que mostrem onde estão e onde são necessárias melhorias e que podemos então atender a tais necessidades com a utilização da TI trabalhando com estudos de Benchmarking, fornecimento de objetivos e métricas dos processos de TI, cumprimento dos objetivos das atividades de TI e avaliação da maturidade do processo de capacidade tudo dentro da própria Governança de TI.

E como isso é feito? Bem, isso tudo é feito com o atendimento da TI a algumas áreas foco:

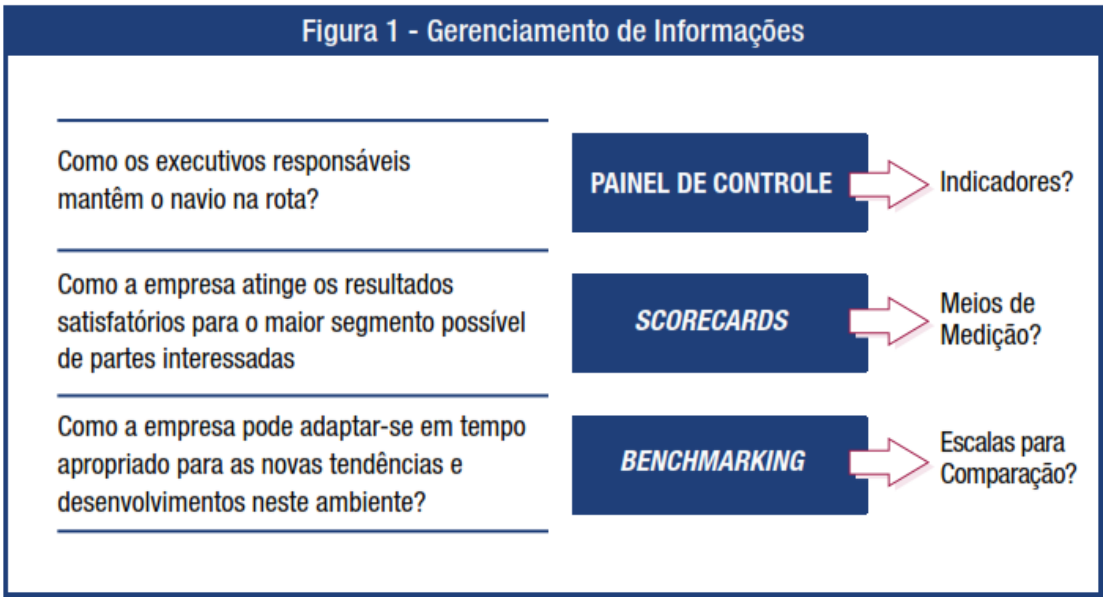
- Tópicos que os executivos precisam atentar para direcionar a área de TI.
- Gerentes operacionais usam os processos para organizar e gerenciar as atividades contínuas de TI.

2 O que é o Cobit?

E neste contexto vem então o Cobit provendo um modelo de processo genérico que representa todos os processos normalmente encontrados nas funções de TI, fornecendo assim um modelo de referência comum compreendido por gerentes operacionais de TI e gerentes de negócios, como foco nas áreas (áreas foco):

- Alinhamento Estratégico: ligação entre plano de negócio e TI.
- Entrega de Valor: TI entrega os prometidos benefícios previstos na estratégia da organização.
- Gestão de recursos: melhor utilização possível.
- Gestão de riscos: riscos assumidos e delegados aos funcionários mais experientes.
- Mensuração de desempenho: acompanha e monitora a implementação da estratégia.

Figura 1 - Gerenciamento de Informações



O Cobit Suporta a Governança de TI com metodologia para assegurar que:

- A área de TI esteja alinhada com os negócios.
- A área de TI habilite o negócio e maximize os benefícios.

- Os recursos de TI sejam usados responsavelmente.
- Os riscos de TI sejam gerenciados apropriadamente.

O Cobit é focado em fazer a ligação, fechar um relacionamento entre a TI e os requisitos de negócio, organizar as atividades de TI em um modelo de processos geralmente aceito, identificar os mais importantes recursos de TI a serem utilizados e definir os objetivos de controle gerenciais a serem considerados.

Tem como características, que serão alvo de algumas explanações maiores sobre cada uma delas logo adiante:

- Focado no negócio.
- Orientado para processos (Possui 4 domínios e 34 processos orientados a TI).
- Baseado em controles (Trabalha com indicadores e fornece controle sobre os processos da TI para o negócio).
- Orientado por medições.

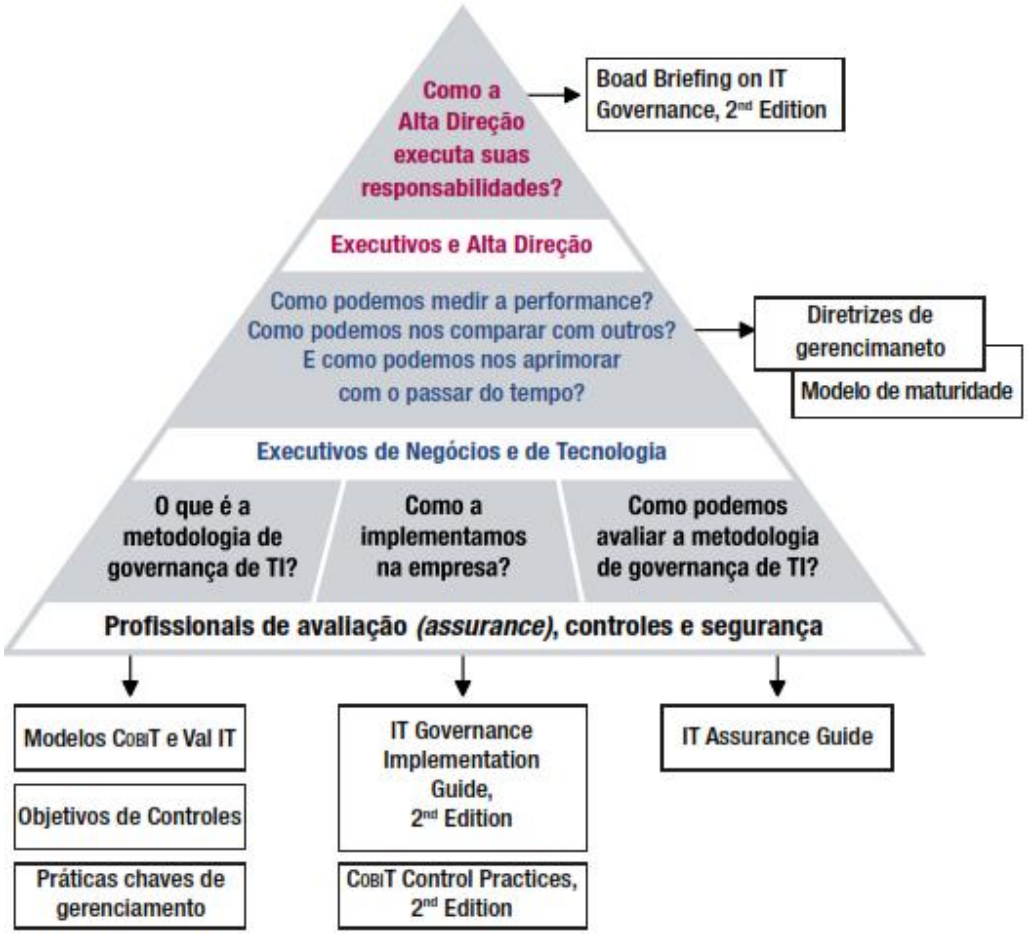
Seu modelo de apresentação pode ser visto como um integrador entre:

- COSO.
- CMMI.
- ITIL.
- Pmbok®.
- Família ISO/IEC 27000.
- Information Security Forum (ISF).
- IT Control Objectives for Sarbanes-Oxley.

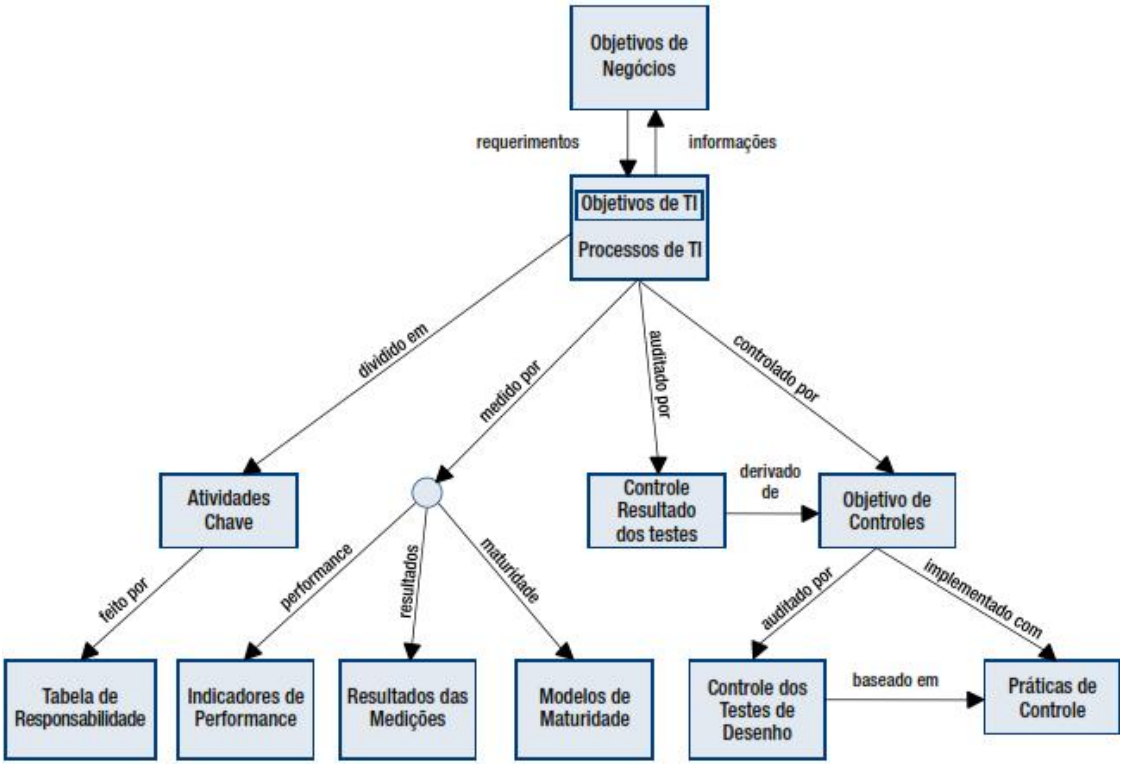
2.1 Modelo Cobit.

Os produtos do Cobit são organizados em 3 níveis, como pode ser verificado na ilustração abaixo:

- Executivos e Alta Direção.
- Gerentes de TI e de negócios.
- Profissionais de avaliação, controles e segurança.



Apresenta sua estrutura com todos os seus componentes inter-relacionados onde podemos ver que ele é atualizado continuamente, visto estar harmonizado com outros padrões e guias e também ser um grande integrador de boas práticas e também ter uma grande garantia de sua estrutura de processos com seu enfoque de alto nível orientado ao negócio e uma visão geral de auxílio á tomada de decisões por parte da alta-direção.



2.2 Vantagens na Implementação do Cobit.

- Melhor alinhamento baseado no foco do negócio.
- Visão clara para os executivos sobre o que TI faz.
- Clara divisão das responsabilidades baseada na orientação para processos.
- Aceitação geral por terceiros e órgãos reguladores.
- Entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum.
- Cumprimento dos requisitos do COSO para controle do ambiente de TI.

2.3 Missão do Cobit:

"Pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação."

2.4 Focado em negócios.

Conforme disse anteriormente, tomaríamos tal assunto para trabalhar um pouquinho melhor em um tópico separado, não somente este tópico presente, mas também a sua orientação a processos e também de ser baseado em controles, conforme os dois itens subseqüentes.

O Cobit apresenta alguns princípios:

- Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir.
- Gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.

Possui em seu modelo uma presença marcante do gerenciamento e controle da informação e por tal motivo vamos dar uma olhadinha quais são os critérios utilizados em relação à informação aqui dentro do Cobit, lembrando que informação é um ativo para a organização.

Critérios de Informação.

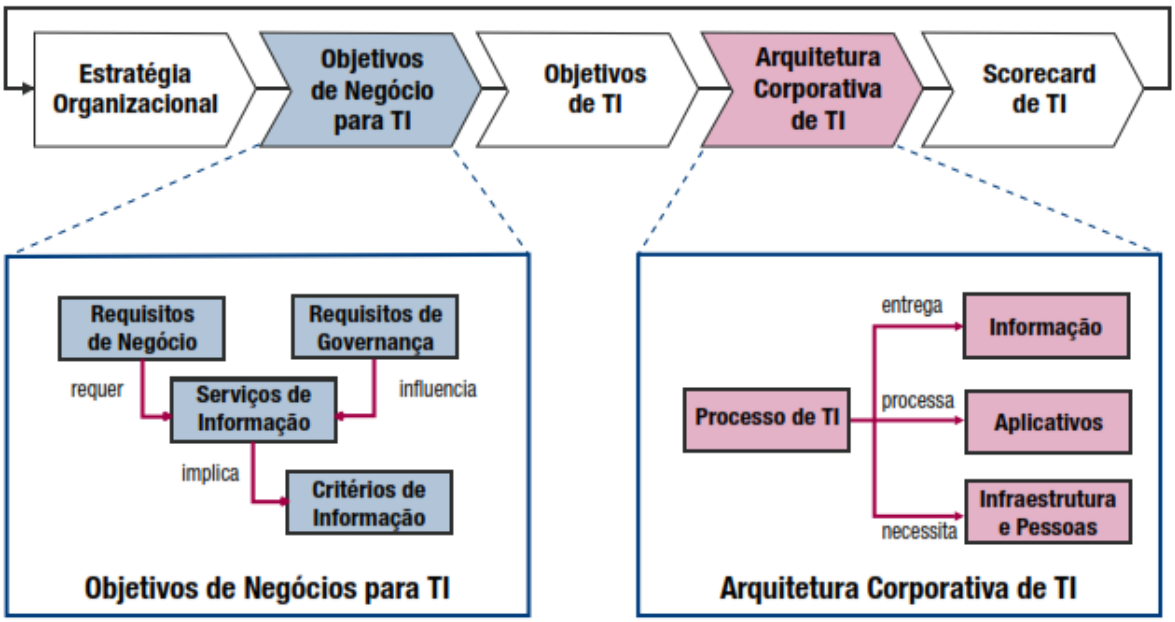
- Efetividade: Informação relevante, pertinente e sendo entregue em tempo de maneira correta, consistente e utilizável.
- Eficiência: Melhor uso dos recursos.
- Confidencialidade: Divulgação indevida.
- Integridade: Fidedignidade e totalidade da informação e validade de acordo com o negócio.
- Disponibilidade: Disponibilidade da informação quando exigida. Salvaguarda dos recursos necessários.
- Conformidade: Aderência às leis, regulamentos e obrigações contratuais.
- Confiabilidade: Entrega das informações apropriadas aos executivos.

Vimos então que o Cobit trabalha com a informação, mas afinal de contas, por quê? Bem, este tipo de consideração é feito justamente pelo fato dele ser focado no negócio. Podemos encontrar então a informação como um dos principais ativos da organização e também como fator primordial do negócio.

Seu foco no negócio vai além do tratamento da informação, ele envolve o alinhamento entre objetivos de negócio e objetivos de TI de forma que tenhamos a TI atendendo às reais necessidades do negócio.

Verifiquem a imagem colocada logo abaixo e poderão ver então que a Estratégia Organizacional irá se desdobrar dentro da instituição em Objetivos de Negócio para a TI, que serão desdobrados em Objetivos de TI, que dará origem às necessidades que a instituição terá de uma Arquitetura Corporativa de TI e que irá gerar por final o Scorecard de TI.

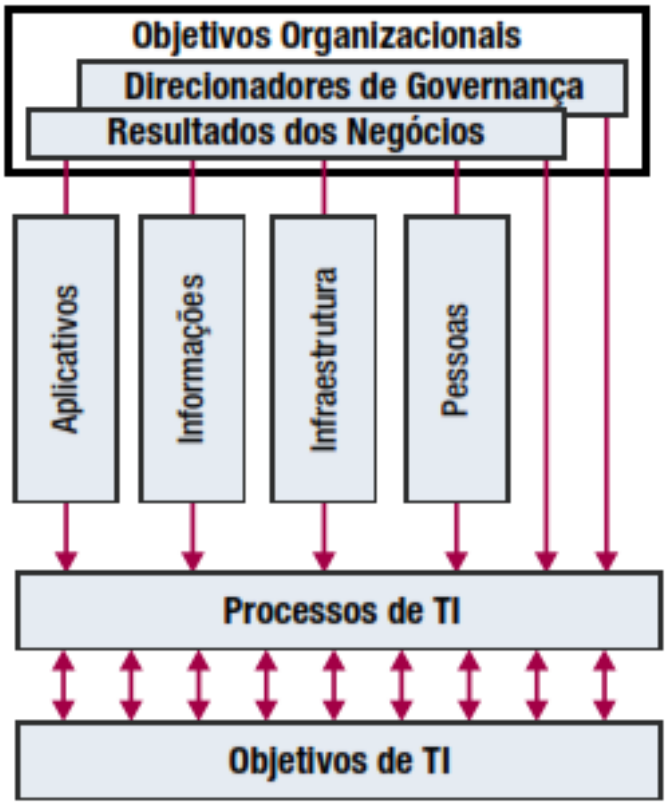
Chama a atenção dos senhores que não são os Objetivos de Negócio para a TI que dão origem direta à Arquitetura Corporativa de TI e sim os Objetivos de TI que o fazem.



Com a estrutura estratégica definida, temos então subsídios para definir quais serão os meus recursos de TI necessários para que tenhamos os

Objetivos de TI dando apoio aos Processos de TI, que por sua vez conseguirão então atender aos Resultados dos Negócios esperados. Os recursos de TI se subdividem em:

- Aplicativos: Sistemas automatizados.
- Informações: Dados em todas as suas formas.
- Infra-estrutura: Tecnologia e os recursos.
- Pessoas: Funcionários internos, terceirizados ou contratados.

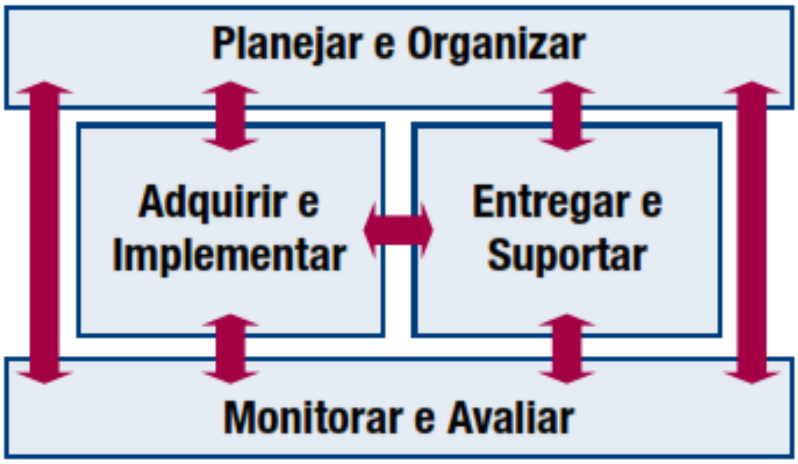


2.5 Orientado para processos.

Conforme já vimos anteriormente, o Cobit também é Orientado para processos certo? Processos estes que são divididos em quatro domínios, conforme abaixo:

- PO (Planejar e Organizar) - Provê direção para entrega de soluções (AI) e entrega de serviços (DS).
- AI (Adquirir e Implementar) - Provê as soluções e as transfere para tornarem-se serviços.

- DS (Entregar e Suportar) - Recebe as soluções e as tornam passíveis de uso pelos usuários finais.
- ME (Monitorar e Avaliar) - Monitora todos os processos para garantir que a direção definida seja seguida.



2.5.1 Planejar e Organizar (PO)

Cobre estratégias e táticas de TI para atingir os objetivos de negócios. Responde às seguintes perguntas:

- As estratégias de TI e de negócios estão alinhadas?
- A empresa está obtendo um ótimo uso dos seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são entendidos e estão sendo gerenciados?
- A qualidade dos sistemas de TI é adequada às necessidades de negócios?

2.5.2 Adquirir e Implementar (AI)

Soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, implementas e integradas ao processo de negócios. Responde às seguintes perguntas:

- Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
- Os novos projetos serão entregues no tempo e orçamento previstos?
- Os novos sistemas ocorreram apropriadamente quando implementado?
- As alterações ocorrerão sem afetar as operações de negócios atuais?

2.5.3 Entregar e Suportar (DS)

Entrega de serviço, gerenciamento da segurança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais. Responde às seguintes perguntas:

- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
- Os custos de TI estão otimizados?
- A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?
- Os aspectos de CID estão sendo contemplados para garantir a segurança da informação?

2.5.4 Monitorar e Avaliar.

Gerenciamento da *performance*, do monitoramento do controle interno, da aderência regulatória e da governança. Responde às seguintes perguntas:

- A performance de TI é mensurada para detectar problemas antes que seja muito tarde?
- O gerenciamento assegura que os controles internos sejam efetivos e eficientes?

- O desempenho da TI pode ser associado aos objetivos de negócio?
- Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

2.6 Baseado em Controles.

A última característica marcante do Cobit é que ele é baseado em controles, trabalha então com a definição de objetivos de controle para todos os seus 34 processos que possuem as seguintes características:

- Considerados pelos executivos:
  - São definições de ações gerenciais para aumentar o valor ou reduzir o risco.
  - Consistem em políticas, procedimentos, práticas e estruturas organizacionais·
  - São desenvolvidos para prover uma razoável garantia de que os objetivos de controle serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos.

Os objetivos de controle de TI fornecem um conjunto completo de requisitos de alto nível a serem considerados pelos executivos para um controle efetivo de cada processo de TI.

O Cobit oferece um modelo de processo genérico de controle compreensível para os gerentes das operações de TI e de negócios e que realiza a ligação entre requisitos de governança, processos e controles de TI.

Dentro de sua estrutura os objetivos de controle são identificados por:

- Letras do domínio.
- Número de processo.
- Número de objetivo de controle.

Cada processo possui requisitos de controle genéricos [PC(n)] que devem ser considerados junto com os objetivos de controle dos processos para uma visão completa dos requisitos de controle.

- PC 1 Metas e objetivos de controle: Assegura que os processos estejam ligados aos objetivos de negócios e que são suportados por métricas apropriadas. Define e comunica as metas e objetivos de controle (SMARRT):
  - Específicos.
  - Mensuráveis.
  - Acionáveis.
  - Realísticos.
  - Orientados a resultados.
  - Tempo apropriado.
- PC 2 Propriedade dos processos: Designa um proprietário para cada processo de TI e claramente define os papéis e responsabilidades de cada proprietário de processo.
- PC3 Repetibilidade dos Processos: Elabora e estabelece cada processo-chave de TI de maneira que possa ser repetido e produzir de maneira consistente os resultados esperados
- PC4 Papéis e Responsabilidades: Define as atividades-chaves e as entregas do processo.
- PC5 Políticas Planos e Procedimentos: Define e comunica como todas as políticas, planos e procedimentos que direcionam os processos de TI são documentados, revisados, mantidos, aprovados, armazenados, comunicados e utilizados para treinamento.

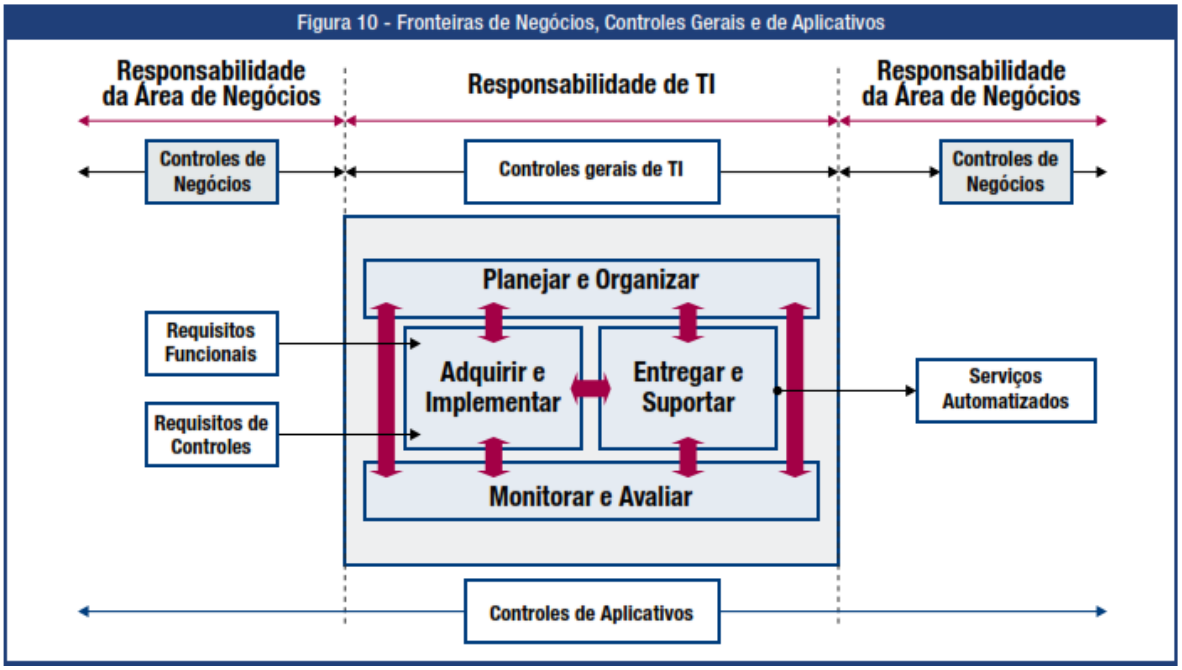
- PC6 Melhoria do Processo de Performance: Identifica um conjunto de métricas que fornecem direcionamento para os resultados e performance dos processos.

Controles efetivos irão reduzir riscos, aumentar a probabilidade da entrega de valor e aprimorar a eficiência.

Dentro da conceituação de controle ainda temos os controles de negócio de TI e os controles gerais de TI e controles de aplicativos:

- Controles de negócio de TI alimentam a alta direção com informações que irão propiciar melhores decisões e definições sobre o negócio, trabalham com controles diretos nos processos de negócio medindo com a área de TI está fornecendo os serviços de TI.
- Controles gerais de TI e Controles de aplicativos:
  - Controles automatizados em aplicativos são da área de TI.
  - Controle e gerenciamento operacional dos aplicativos são do proprietário do negócio.

Figura 10 - Fronteiras de Negócios, Controles Gerais e de Aplicativos



Para melhor entendimento observe a imagem acima e vejam em gráfico onde cada um dos controles entra. Verão então que os controles automatizados em aplicativos são de responsabilidade da TI e que os controles de negócios ficam a cargo da Área de Negócio.

Vejamos abaixo uma lista de objetivos de controles de aplicativos.

- AC1 Preparação e Autorização de Dados Originais.
    - Assegura que os documentos fonte sejam preparados por pessoal autorizado e qualificado seguindo os procedimentos estabelecidos, levando em consideração uma adequada segregação de funções relacionadas com a criação e aprovação desses documentos.
- AC2 Entrada e Coleta de Dados Fontes.
    - Estabelece que a entrada de dados seja executada de maneira apropriada por pessoal autorizado e qualificado.
- AC3 Testes de Veracidade, Totalidade e Autenticidade.
    - Assegura que as transações sejam exatas, completas e válidas.
- AC4 Processamento Íntegro e Válido.
    - Mantém a integridade e validade dos dados no ciclo de processamento.
- AC5 Revisão das Saídas, Reconciliação e Manuseio de Erros
    - Estabelece procedimentos e responsabilidades associadas para assegurar que as saídas sejam manuseadas de uma forma autorizada, entregues para os destinatários corretos e protegidas durante a transmissão.
- AC6 Autenticação e Integridade das Transações
    - Verifica endereçamento adequado, autenticidade da origem e integridade do conteúdo.

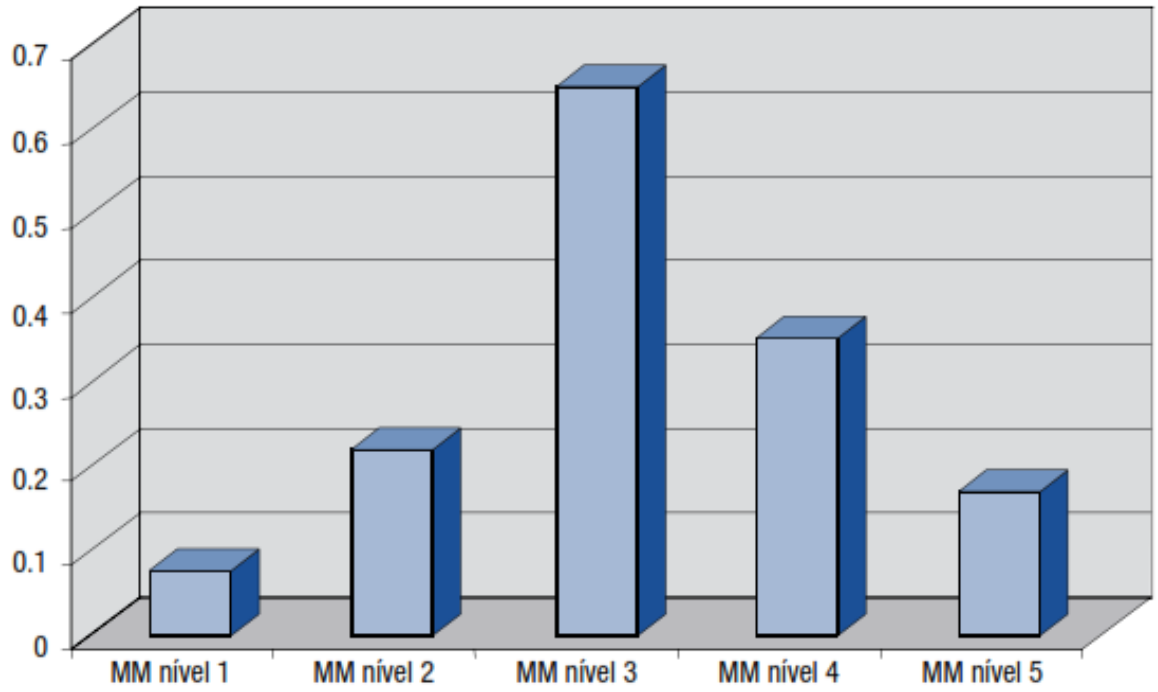
2.7 Direcionamento baseado em medição.

"O quão distante devemos ir e será que o custo é justificado pelo benefício?"

Conforme venho reforçando em várias citações feitas nesta matéria, o Cobit é Baseado em medições e isto é bem interessante de ser observados, pois sabemos que tudo que é medido pode ser quantitativamente e qualitativamente melhorado e é justamente desta idéia que surge um modelo de maturidade baseado no CMM e adotado dentro do Cobit.

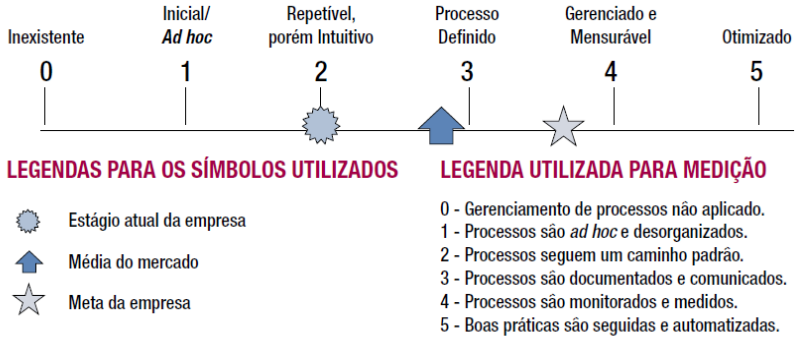
- Tudo começa com respostas a:
    - Onde a empresa está?
    - Para onde a empresa quer ir?
    - Progresso em relação às metas?

Sua avaliação é feita de 0 (não existente) a 5 (otimizado) e vai se diferenciar de outros modelos de maturidade devido ao fato de não haver a intenção de medir os níveis de maneira exata ou tentar certificar que um nível foi exatamente atingido. Tem como objetivo resultar em um perfil em que as condições relevantes para diversos níveis de maturidade serão atingidas.



- 0 inexistente – Completa falta de um processo reconhecido.
- 1 inicial / Ad hoc – Existe evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado.
- 2 repetível, porém intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa.
- 3 Processo definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento.
- 4 Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando bem.
- 5 Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações.

Figura 12 - Representação Gráfica dos Modelos de Maturidade



2.8 MEDIÇÃO DE PERFORMANCE.

Definido em três níveis:

- Objetivos e métricas de TI que definem o que os negócios esperam de TI e como medir isso.
- Objetivos e métricas dos processos que definem o que os processos de TI precisam entregar para suportar os objetivos de TI e como medir isso.
- Objetivos e métricas de atividades que estabelecem o que precisa acontecer dentro do processo para atingir a requerida performance e como medir isso

Os objetivos de negócio irão definir vários objetivos de TI que irão suportá-los enquanto o objetivo de TI será atingido por um processo ou por interação de um determinado número de processos.

Devemos observar que já nesta nova versão do Cobit, a 4.1 os termos KGI e KPI foram substituídos, fiquem atentos a isso na sua prova e eles agora se chamam:

- KGIs: Medidas de Resultados.
- KPIs: Indicadores de performance.

As medidas de resultados (saídas) indicam se os objetivos foram atingidos. *(lag indicators)* e os indicadores de performance indicam se os objetivos serão possivelmente atingidos. *(lead indicators),* ou seja,

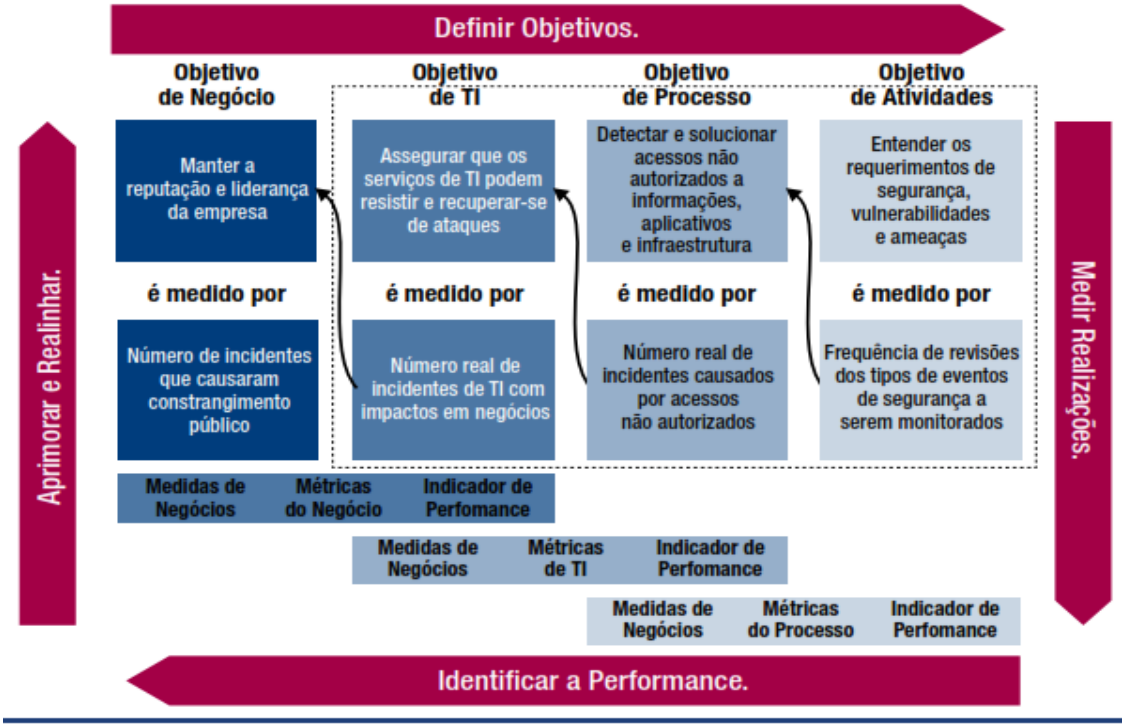
medidas de resultados medidos depois e indicadores de performance medidos antes.

Vejamos abaixo então algumas relações que podem ser feitas entre Medidas de resultados e Indicadores de Performance e que acredito ser objeto de questão na tua prova:

- No nível menor as medidas de resultados tornam-se indicadores de performance para o nível maior.
- As medidas de resultados definem as medições que informam a gerência se a função, os processos e a atividade de TI atingiram seus objetivos.
- As medidas de resultados não são fornecidas para objetivos de negócio.
- Os indicadores de performance definem medidas que determinam quão bem as coisas estão.

Segue abaixo um gráfico encontrado no Cobit 4.1 que ilustra o relacionamento entre objetivos de negócio, TI, processos e atividades e suas respectivas métricas, reparem que os objetivos foram propositalmente colocados em cascata (Objetivos de Negócio para Objetivo de Atividades). Este exemplo gráfico é baseado na DS 5 Garantir a segurança dos serviços.

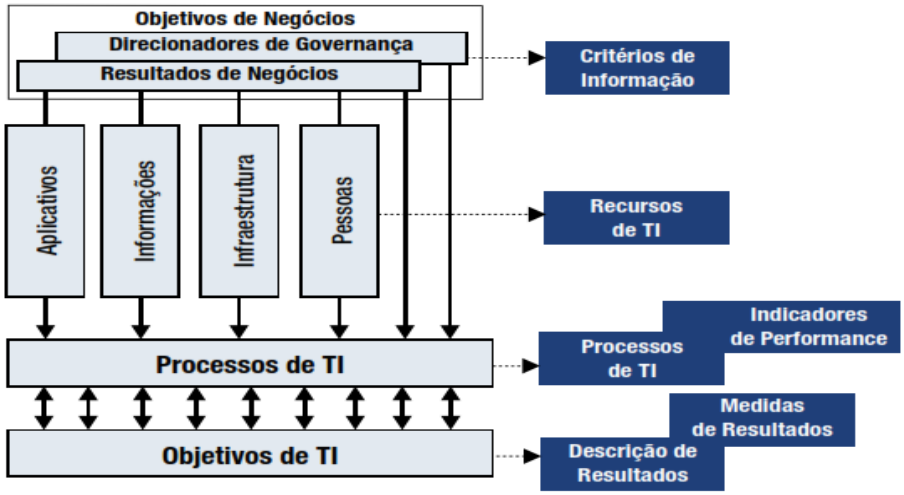
Figura 19 - Relacionamento entre Processos, Objetivos e Métricas (DS5)



2.9 Estrutura do Modelo Cobit.

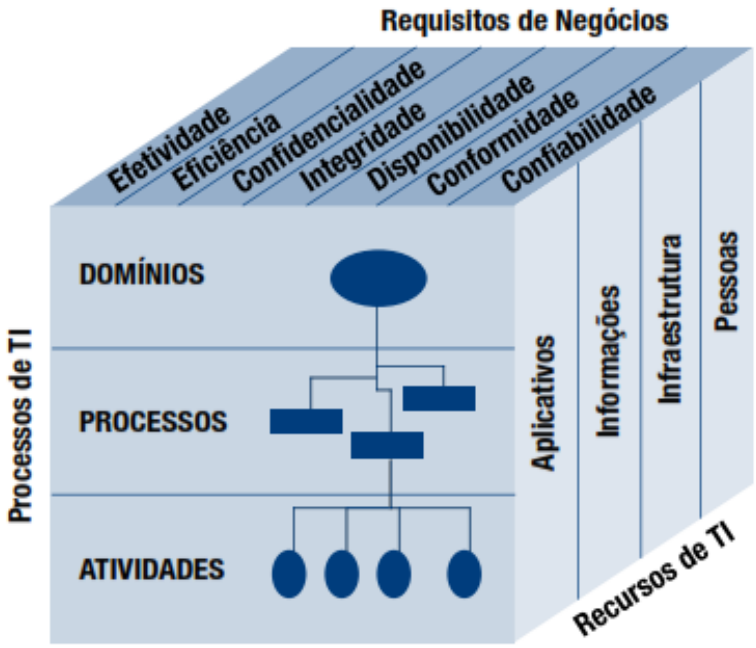
"O modelo Cobit une os requisitos de negócios para informação e governança aos objetivos da função de serviços de TI. O modelo de processos do Cobit permite que as atividades de TI e os recursos que as suportam sejam serem apropriadamente gerenciados e controlados com base nos objetivos de controle de Cobit, bem como alinhados e monitorados usando os objetivos e métricas do Cobit". (Cobit 4.1)

Figura 21 - Gerenciamento, Controle, Alinhamento e Monitoramento do CobiT



"Em resumo, os recursos de TI são gerenciados pelos processos de TI para atingir os objetivos de TI que respondem aos requisitos de negócios." (Cobit 4.1)

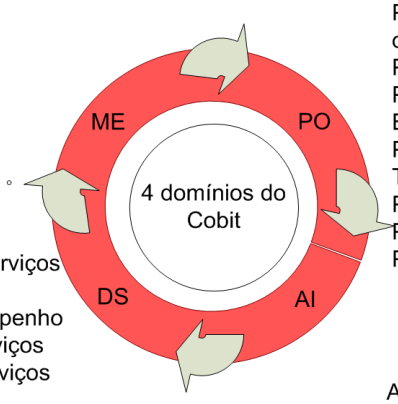
Figura 22 - Figura do CobiT



Como os senhores já sabem, adoro apresentar alguns quadrinhos mágicos e abaixo já encaminho um com todos os processos do Cobit 4.1 e cabe aos senhores repassarem esta imagem para o papel, desenhar manualmente, pregar onde mais vejam, enfim, forcem sua memória fotográfica para trabalhar com ela.

ME1 Monitorar e Avaliar o Desempenho
ME2 Monitorar e Avaliar os Controles Internos
ME3 Assegurar a Conformidade com Requisitos Externos
ME4 Prover a Governança de TI

PO1 Definir um Plano Estratégico de TI
P02 Definir a Arquitetura da Informação
PO3 Determinar o Direcionamento Tecnológico
PO4 Definir os Processos, Organização e os Relacionamentos de TI
PO5 Gerenciar o Investimento de TI
PO6 Comunicar as Diretrizes e Expectativas da Diretoria
PO7 Gerenciar os Recursos Humanos de TI
PO8 Gerenciar a Qualidade
PO9 Avaliar e Gerenciar os Riscos de TI
PO10 Gerenciar Projetos



DS1 Definir e Gerenciar Níveis de Serviços
DS2 Gerenciar Serviços de Terceiros
DS3 Gerenciar Capacidade e Desempenho
DS4 Assegurar Continuidade de Serviços
DS5 Assegurar a Segurança dos Serviços
DS6 Identificar e Alocar Custos
DS7 Educar e Treinar os Usuários
DS8 Gerenciar a Central de Serviço e os Incidentes
DS9 Gerenciar a Configuração
DS10 Gerenciar os Problemas
DS11 Gerenciar os Dados
DS12 Gerenciar o Ambiente Físico
DS13 Gerenciar as Operações

AI1 Identificar Solução Automatizadas
AI2 Adquirir e Manter Software Aplicativo
AI3 Adquirir e Manter Infraestrutura de Tecnologia
AI4 Habilitar Operação e Uso
AI5 Adquirir Recursos de TI
AI6 Gerenciar Mudanças
AI7 Instalar e Homologar Soluções e Mudanças

Bem gente, digo que 70% das questões da sua prova serão baseadas no que foi apresentado até agora, mas sei também que para vocês gabaritarem tal disciplina precisarão conhecer os outros 30%, então vou apresentar para os senhores todos os 34 processos do Cobit abaixo e fazer alguns comentários sobre aqueles que possuem maior probabilidade de serem cobrados nas suas provas.

Infelizmente é um processo de decoreba aplicado mesmo, ou seja, é pegar, ler o conteúdo, anotar os pontos mais importantes e correr pro abraço.

Trabalharei com os senhores no que realmente irá fazer com que os senhores identifiquem o processo de TI citado: o seu foco e como ele é alcançado.

3 Planejar e Organizar.

O domínio Planejar e Organizar possui 10 processos sendo que deles eu gostaria que os senhores se atentassem mais ao PO9 por se tratar exatamente do conteúdo adicional solicitado em seu edital e como tal trataremos dele de forma detalhada, ao contrário dos demais processos, os quais iremos trabalhar somente com a citação de seus nomes (lembrem-se, estamos falando de noções de Cobit e acredito realmente que a cobrança dos processos na integra e dos objetivos de controle fujam a tal expectativa).

Minha visão é de na verdade cobrarem o que temos do Cobit em relação a processos que estão alinhados com Licitações e Contratos de TI.

- PO1 Definir um Plano Estratégico de TI.
- PO2 Definir a Arquitetura da Informação.
- PO3 Determinar as Diretrizes de Tecnologia.
- PO4 Definir os Processos, a Organização e os Relacionamentos de TI.
- PO5 Gerenciar o Investimento de TI.
- PO6 Comunicar Metas e Diretrizes Gerenciais.
- PO7 Gerenciar os Recursos Humanos de TI.
- PO8 Gerenciar a Qualidade.
- PO9 Avaliar e Gerenciar os Riscos de TI.
- PO10 Gerenciar Projetos.

3.1 PO9 Avaliar e Gerenciar os Riscos de TI

Tem como objetivo criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de

TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.

Com foco em:

- Desenvolver uma estrutura de gerenciamento de risco integrada às estruturas corporativa e operacional de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual.

É alcançado por:

- Garantia de que o gerenciamento de risco esteja completamente integrado aos processos gerenciais, interna e externamente, e seja aplicado de forma consistente.
- Realização de avaliações de risco.
- Recomendação e comunicação de planos de ação de remediação dos riscos.

É medido por:

- Percentual de objetivos críticos de TI cobertos pela avaliação de risco.
- Percentual de riscos críticos de TI identificados que tenham planos de ação desenvolvidos.
- Percentual dos planos de ação de gestão de risco aprovados para implementação.

3.1.1 Objetivos de Controle.

- PO9.1 Alinhamento da gestão de riscos de TI e de Negócios

Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).

- PO9.2 Estabelecimento do Contexto de Risco

  Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.

- PO9.3 Identificação de Eventos

  Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.

- PO9.4 Avaliação de Risco

  Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos.

  A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.

- PO9.5 Resposta ao Risco

  Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.

- PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco

  Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.

4 Adquirir e implementar.

O domínio Adquirir e Implementar é composto por 7

- AI 1 Identificar Soluções Automatizadas.
- AI2 Adquirir e Manter Software Aplicativo.
- AI3 Adquirir e Manter Infraestrutura de Tecnologia.
- AI4 Habilitar Operação e Uso.
- AI5 Adquirir Recursos de TI.
- AI6 Gerenciar Mudanças.
- AI7 Instalar e Homologar Soluções e Mudanças.

5 Entregar e suportar.

O domínio Entregar e Suportar trabalha com 13.

- DS1 Definir e Gerenciar Níveis de Serviços.
- DS2 Gerenciar Serviços Terceirizados.
- DS3 Gerenciar o Desempenho e a Capacidade.
- DS4 Assegurar a Continuidade dos Serviços.
- DS5 Garantir a Segurança dos Sistemas.
- DS6 Identificar e Alocar Custos.
- DS7 Educar e Treinar os Usuários.
- DS8 Gerenciar a Central de Serviço e os Incidentes.
- DS9 Gerenciar a Configuração.
- DS10 Gerenciar Problemas.
- DS11 Gerenciar os Dados.
- DS12 Gerenciar o Ambiente Físico.
- DS13 Gerenciar as Operações.

6 Monitorar e Avaliar.

Ó último domínio a ser tratado no Cobit é o Monitorar e Avaliar que possui 4 processos.

- ME1 Monitorar e Avaliar o Desempenho de TI
- ME2 Monitorar e Avaliar os Controles Internos
- ME3 Assegurar a Conformidade com Requisitos Externos
- ME4 Prover Governança de TI

7 Noções de Riscos em TI.

Sabemos então que no edital dos senhores a banca está cobrando noções de Riscos em Tecnologia da Informação, certo? E como já visto anteriormente o Cobit possui inclusive um dos seus processos orientado justamente à avaliação de riscos. Vamos neste momento tratar de alguns conceitos aplicáveis ao assunto de forma que possam estar os mais bem preparados possíveis para a sua prova.

Existe então a norma NBR ISO/IEC 27.005:2008 que trata do Gerenciamento de Riscos de uma forma geral, mas que possui toda a sua conceituação aplicável ao nosso assunto que é Riscos em Tecnologia da Informação, então vamos utilizá-la como material base para o presente conteúdo.

Primeiro de tudo vamos tratar de alguns conceitos necessários para entendermos o mini-mundo no qual o assunto Riscos está envolvido.

7.1 Ativo.

Tudo que tenha valor e que necessite de algum tipo de proteção ou cuidado, sua identificação adequada é atividade fundamental para o estabelecimento de qualquer estratégia de proteção e de implementação de GR.

7.2 Ameaça.

Tudo que tem potencial de causar algum tipo de dano a um ativo, temos ainda desta definição que um incidente é uma ameaça concretizada. Reparem bem que uma ameaça irá explorar as vulnerabilidades presentes na organização. Pode ter origem:

- Ambiental: causada por fenômenos naturais, interrupções de serviços básicos (energia elétrica, telefonia), ou até mesmo desastres ou incêndios.

- Humana: causada diretamente pela ação humana, ação de pessoas que pode ainda ser dividida em ações humanas acidentais e intencionais (e neste caso fica bem claro o que significa cada uma né).

Obs.: Uma ameaça pode afetar mais de um ativo.

7.3 Vulnerabilidade.

São fraquezas que acabam criando situações que poderão ser explorados por ameaças, sua existência por si só não causa prejuízo.

Seu processo de identificação das proteções existentes e ausentes, identificação das falhas e levantamento de dados que posam prever a efetividade do definido conjunto de proteção é chamado de análise de vulnerabilidades. Quando combinamos tal análise com um conjunto de prováveis ameaças daí já estamos falando de avaliação de vulnerabilidades (prestem muita atenção nestas duas definições, pois estão presentes na norma e caem na prova).

7.4 Proteção.

São práticas, procedimentos, mecanismos ou ferramentas que podem proteger os ativos contra ameaças, mitigar ou eliminar vulnerabilidades, diminuir o impacto de um incidente e até mesmo detectar sua existência.

Vemos então que praticamente todas as estratégias adotadas em segurança da informação se fundamentam na utilização de proteções adequadas.

7.5 Risco.

Um dos principais focos da nossa aula de hoje né? Então não preciso nem dizer que os senhores devem neste exato momento ligar o turbo de concentração né?

Trata-se da probabilidade de uma ameaça explorar uma ou mais vulnerabilidades causando prejuízos aos ativos da organização, estão sempre relacionados à ocorrência de incidentes e neste momento temos então a consideração mais abrangente sobre o assunto, pois aqui estaremos tratando os riscos com características negativas ou positivas**,** ou seja, trazendo prejuízos aos ativos da organização ou benefícios, sendo que a organização tratará deste risco de forma a evitá-lo, transferi-lo, rete-lo ou reduzi-lo.

Sua escala de criticidade para a organização será dada pela combinação (produto, multiplicação, X, *) de dois fatores, a probabilidade de sua ocorrência e as conseqüências trazidas pela ocorrência do incidente (impacto).

Risco = Probabilidade X Impacto.

Temos duas características muito fortes quando falamos em risco para a Gestão de Riscos - GR, o primeiro é que riscos que podem ser completamente eliminados geram sobras chamadas de risco residual, a segunda é que a GR se preocupa em trazer estes riscos residuais para dentro de patamares aceitáveis, que serão definidos pelo critério de risco da organização, tratando com o conceito do que seria tolerável ou não para ela em relação ao risco e seus impactos aos ativos prioritários.

Vemos então que na GR e de acordo com a própria 27005 nós temos 4 etapas/formas de lidar com riscos (ciclo de vida de um risco):

- Avaliação de risco.
- Tratamento de risco.
- Aceitação de risco.
- Comunicação de risco.

7.6 Percepção de Risco.

É a forma como o risco é percebido ou visto por uma parte envolvida e pode variar de acordo com os critérios, valores, prioridades e interesses utilizados (risco percebido).

7.7 Gestão de Riscos.

É uma série de atividades relacionadas à forma como a organização irá tratar os riscos, trata de todo o ciclo de vida de um risco.

7.8 Análise e Avaliação de Risco (AAR).

Vem do inglês *Risk Assesment* e a sua primeira definição análise (risk analysis) trata da identificação de ameaças (*threat identification*) e estimativa do risco (*risk estimation*), já a avaliação (*risk evaluation*) trata de comparar os riscos que foram previamente identificados e estimados com os critérios de risco definidos pela organização.

Risco
- Probabilidade.
- Evento
- Conseqüência.

7.9 Tratamento.

Segunda fase da GR tem como objetivo a seleção e implementação de medidas de forma a reduzir os riscos negativos. Podem ser:

- Evitar: neste caso a instituição estará preocupada em não se envolver ou não se expor a uma situação de risco, simplesmente tentará evitá-lo.
- Transferir: caso clássico da contratação de um seguro, na qual o responsável pelo risco transfere o impacto dele, mas ainda permanece responsável pelo seu monitoramento. Está relacionado ao ônus da perda ou ao benefício do ganho. Em segurança da informação somente riscos negativos são considerados para efeitos de transferência.
- Reter: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado. (04/IN01/DSIC/GSIPR/Presidência da República). Aceitação do ônus da perda ou do benefício do ganho.
- Reduzir: Implementar algum tipo de proteção que reduza a probabilidade ou o impacto negativo do risco, caso mesmo assim ocorra, acaba por gerar risco residual.

7.10 Aceitação.

Deverá ocorrer somente quando o custo de proteção contra um determinado risco não valha a pena, ou seja, custo de proteção maior que o do ativo ou muito próximo dele. Pode ocorrer também quando o risco já se encontra dentro do critério de risco. Em sua essência, atua como o definido em reter o risco.

7.11 Sistema de Gestão de Riscos (SGR).

Trata-se do conjunto de elementos e funções relacionadas ao gerenciamento de riscos que compõe o sistema de gestão da organização.

Comportam o planejamento estratégico, o processo decisório e outros processos relacionados ao risco, possui então metas e objetivos

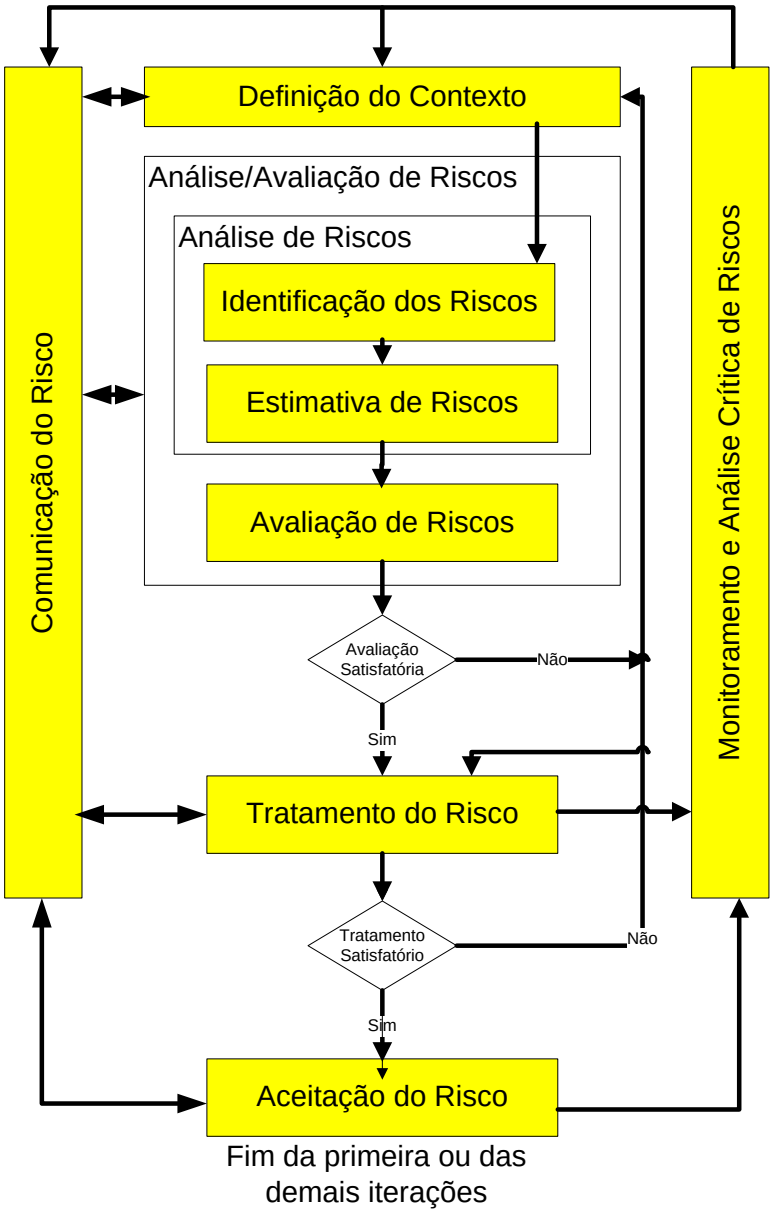
previamente definidos, o que nos força a trabalhar com um planejamento prévio incorporando os objetivos ao sistema e os alinhando ao negócio da organização.

7.12 Apetite a risco.

Quantidade total de risco que uma organização está preparada para aceitar, tolerar ou ser exposta a qualquer tempo.

7.13 Visão geral do processo de gestão de riscos de segurança da informação.

Ele consiste basicamente na definição do contexto, na análise/avaliação dos riscos (AAR), no tratamento de risco, aceitação de risco, comunicação do risco e monitoramento e análise crítica de riscos, conforme gráfico abaixo.



Como pode ser verificado, tudo começa com a definição do contexto, logo em seguida deve ser executada a análise/avaliação de riscos, se ela

fornecer informações suficientes, pronto, segue então para o tratamento do risco, senão o contexto deve ser redefinido.

Observo ainda que as atividades de análise/avaliação de riscos e/ou de tratamento do risco poderão ser realizadas mais de uma vez, visto que mediante enfoque mais iterativo, se torna possível aprofundar e detalhar cada vez mais o risco em cada iteração, fora a capacidade de minimizar o tempo e o esforço necessário para identificação e controle dos riscos.

E por final, devemos levar para a prova que a eficácia do tratamento do risco depende dos resultados da análise/avaliação de riscos.

Vejamos então o que acontece quando se obtêm riscos residuais. Neste caso teremos de considerar que eles deverão estar claramente explícitos e aceitos pelos gestores nos definidos critérios de risco.

Com a visão acima, sabemos então que a aplicação do processo de tratamento de riscos mostrado trabalha neste momento de uma forma ainda genérica, mas nosso foco não é a aplicação de GR em um SGSI? Sim né? Então precisamos voltar tal tipo de conhecimento justamente para nossa área foco e quando fazemos isso temos o alinhamento do processo de gestão de riscos feito diretamente com o ciclo PDCA e logo teremos a seqüência relacional de atividades sendo realizadas.

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Análise/avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Visão geral danada né? Mas se não entendeu, solicito que retorne ao inicio do tópico e tente entender, analise o gráfico apresentado e ainda

complemente mentalmente a necessidade de termos a comunicação de forma efetiva para que tudo isso funcione e como ela entra justamente como ferramenta de suma importância para a gestão de riscos.

Então senhores, o que tinha para lhes apresentar de conteúdo teórico sobre Governança de TI, Noções de Cobit e Riscos era isso, vamos trabalhar com os exercícios que acredito que serão muito uteis para os senhores.

Na continuidade desta aula, e até mesmo para ela não ficar muito extensa, eu publico os exercícios comentados como Aula 05-1.

Utilizem nosso canal aberto de comunicação via e-mail no endereço gabrielpacheco@estrategiaconcursos.com.br no qual (na medida do possível ☺ dúvidas sobre questões e considerações feitas nas aulas poderão ser tiradas, mas reforço que dou preferência ao Fórum criado, assim todos ficam sabendo e podem inclusive participar. Ao enviarem e-mail para este endereço, favor colocarem sempre no campo assunto sobre qual curso, cargo ou concurso está falando.

Caso achem necessária a criação de um fórum de discussão, favor me enviarem e-mail com tal solicitação que crio mesmo fora da estrutura do Estratégia para discutirmos em grupo as dúvidas e questões referentes à nossa disciplina no concurso.

Como deu trabalho para escrever esta aula e todas as outras que virão também vão dar, caso resolva utilizá-la para qualquer fim, favor citar a fonte e também me avisar. J

Lembrem-se sempre, **seu maior adversário é você.**

Abraços a todos!!!!