Governança de TI: O que é COBIT ?

Agenda

- Governança de TI
- Metodologia COBIT
- Relacionamento do COBIT com os modelos de melhores práticas
- Governança de TI em 2006
- Estudo de Caso
- Referências

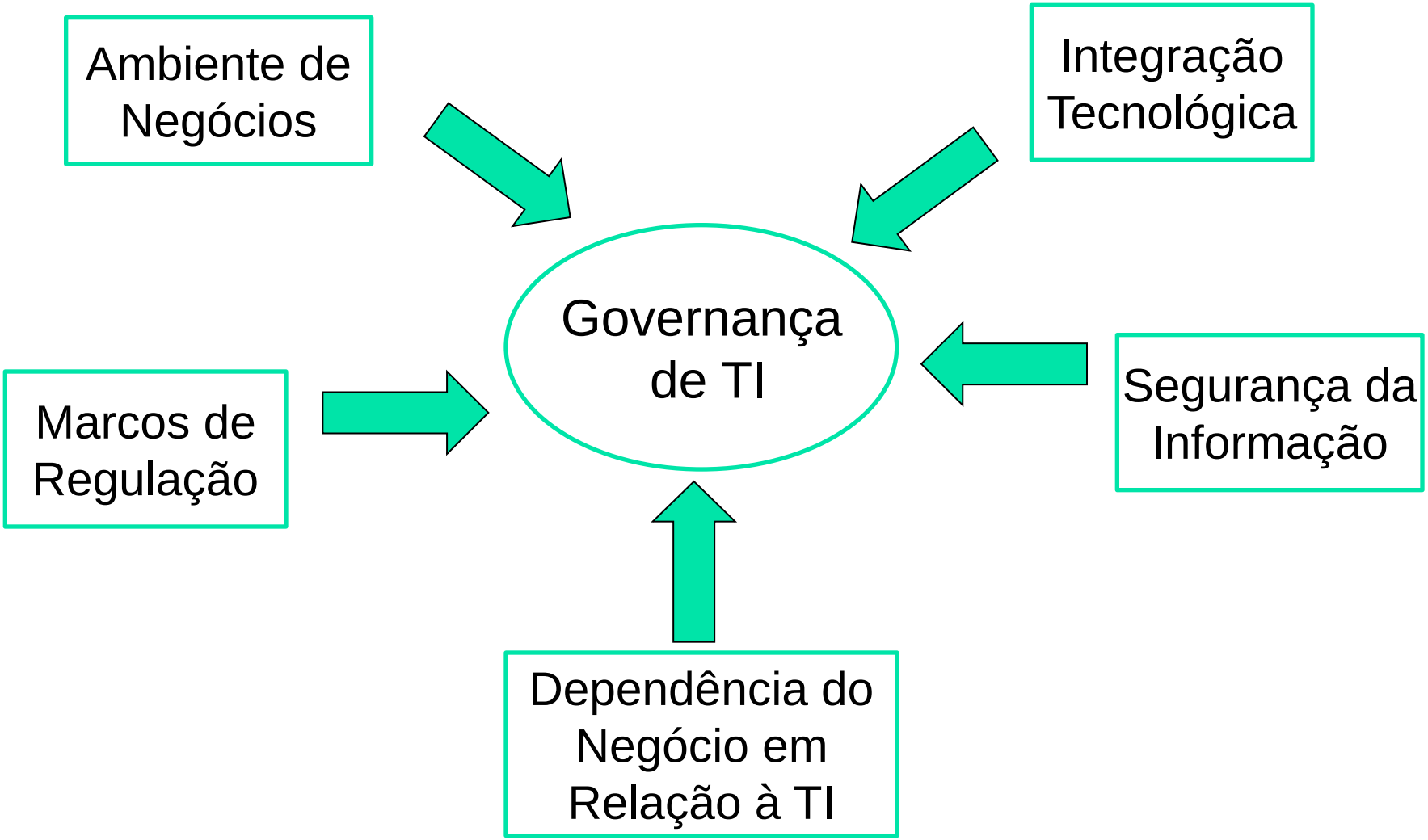
Governança de TI

- **De acordo com o IT Governance Institute (2005)**

  "A governança de TI é de responsabilidade de alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização."

Governança de TI

- Fatores motivadores da Governança de TI



Governança de TI

- Framework para Gerenciamento de TI
  - A Governança de TI, quando implementada de forma integrada:
    - Permite que a empresa gerencie de forma eficiente seus investimentos em recursos tecnológicos e suas informações transformando-as em maximização de benefícios, oportunidades de negócio e vantagem competitiva no mercado.
  - A estrutura do COBIT- Control Objectives for Information and Related Technology – foi idealizada de forma a atender às necessidades de controle da organização relacionadas à Governança de TI.

Histórico do COBIT

- O COBIT foi criado em 1994 pela ISASFC (Information Systems Audit and Control Foundation, ligado à ISACA).
- Em 1998, foi publicada a sua 2ª edição, contendo uma revisão nos objetivos de controle de alto nível e detalhados, e mais um conjunto de ferramentas e padrões para implementação.
- A 3ª edição foi publicada em 2000 pelo IT Governance Institute (ITGI).

Histórico do COBIT

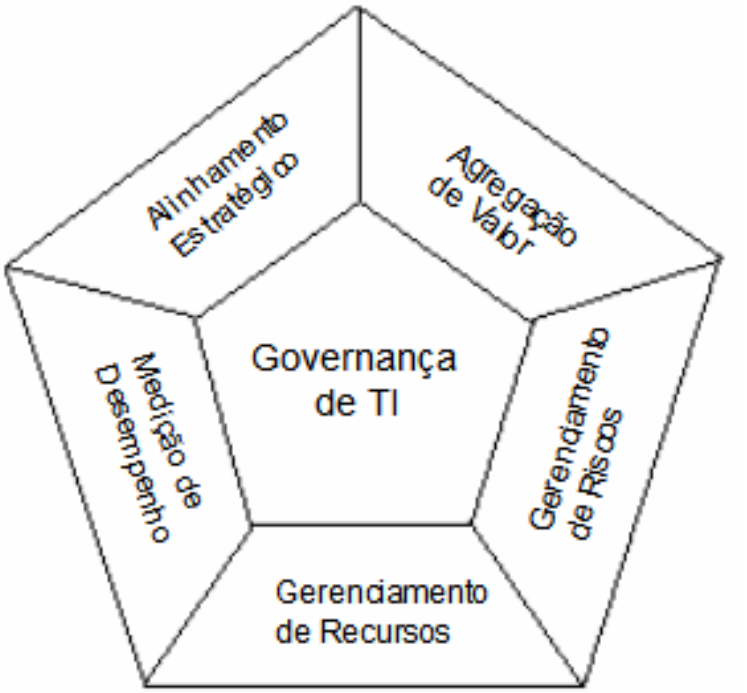
- O modelo evoluiu novamente em 2005 para a versão 4.0, através de práticas e padrões mais maduros.
- O COBIT está em conformidade com as regulamentações, do foco mais acentuado na governança de TI, nos níveis mais elevados e da ampliação da sua abrangência para um público mais heterogêneo (gestores, técnicos, especialistas e auditores de TI).
- COBIT 4.1 -2007

Público Alvo do COBIT

- Gestão Executiva
- Gestão de Negócios
- Gestão de TI
- Auditores

Objetivo do COBIT

- Contribuir para o sucesso da entrega de produtos e serviços de TI, a partir da perspectiva das necessidades do negócio, com um foco mais acentuado no controle que na execução.
- Focos da Governança de TI, na visão do COBIT



Estrutura do COBIT

- Consiste de um conjunto de 210 Controles, organizados em 34 Processos que são agrupados em 4 Domínios, aplicáveis aos sistemas e à TI.
- Principais Características
  - Foco nos requisitos do negócio
  - Orientação para uma abordagem de processos
  - Utilização de mecanismos de controles
  - Direcionamento para a análises das medições e indicadores de desempenho obtidos ao longo do tempo

Estrutura do COBIT

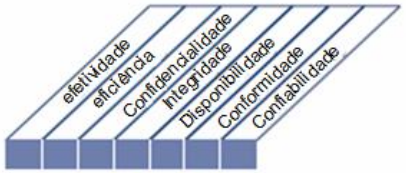
- **Foco no Negócio**
  - Recursos de TI
    - Aplicações, Informação, Infra-estrutura e Pessoas
  - Critérios de Controle
    - Eficiência,Eficácia, Confidencialidade, Integridade, Disponibilidade, Conformidade com regulações(*Compliance*) e Confiabilidade.

Estrutura do COBIT

- Controle através de objetivos
  - Os objetivos de controle do COBIT procuram atestar como cada processo faz uso dos recursos de TI para atender de forma primária ou secundária cada requerimento do negócio em termos de informação, cobrindo todos os seus aspectos:
    - **Primário (P**) – Indica o nível no qual o objetivo de controle definido tem impacto direto no critério de informação.
    - **Secundário (S)** – Indica o nível no qual o objetivo de controle definido apenas satisfaz o critério de informação, podendo ser em pouca extensão ou inclusive indiretamente.
    - **Não Preenchimento** – Poderia ser aplicável, todavia outro critério de avaliação é mais adequado a este processo.

Estrutura do COBIT

- Controle através de objetivos



Controle sobre o processo de TI de

Nome do processo

que satisfaça a exigência do negócio de

resumo dos mais importantes objetivos de negócio

é atingido mediante

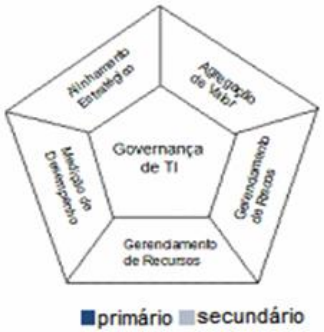
resumo dos mais importantes objetivos de TI

e leva em consideração

controles chaves

e é mensurado por

métricas chaves



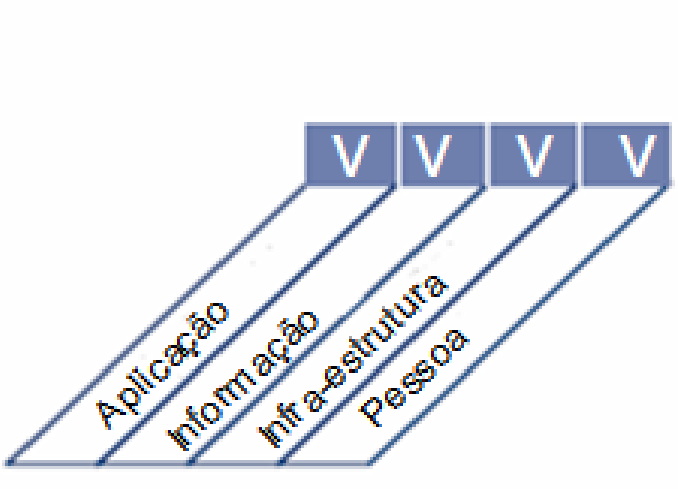
Objetivos de Controle
PO9 – Avaliar e Gerenciar os Riscos de TI

é atingido mediante

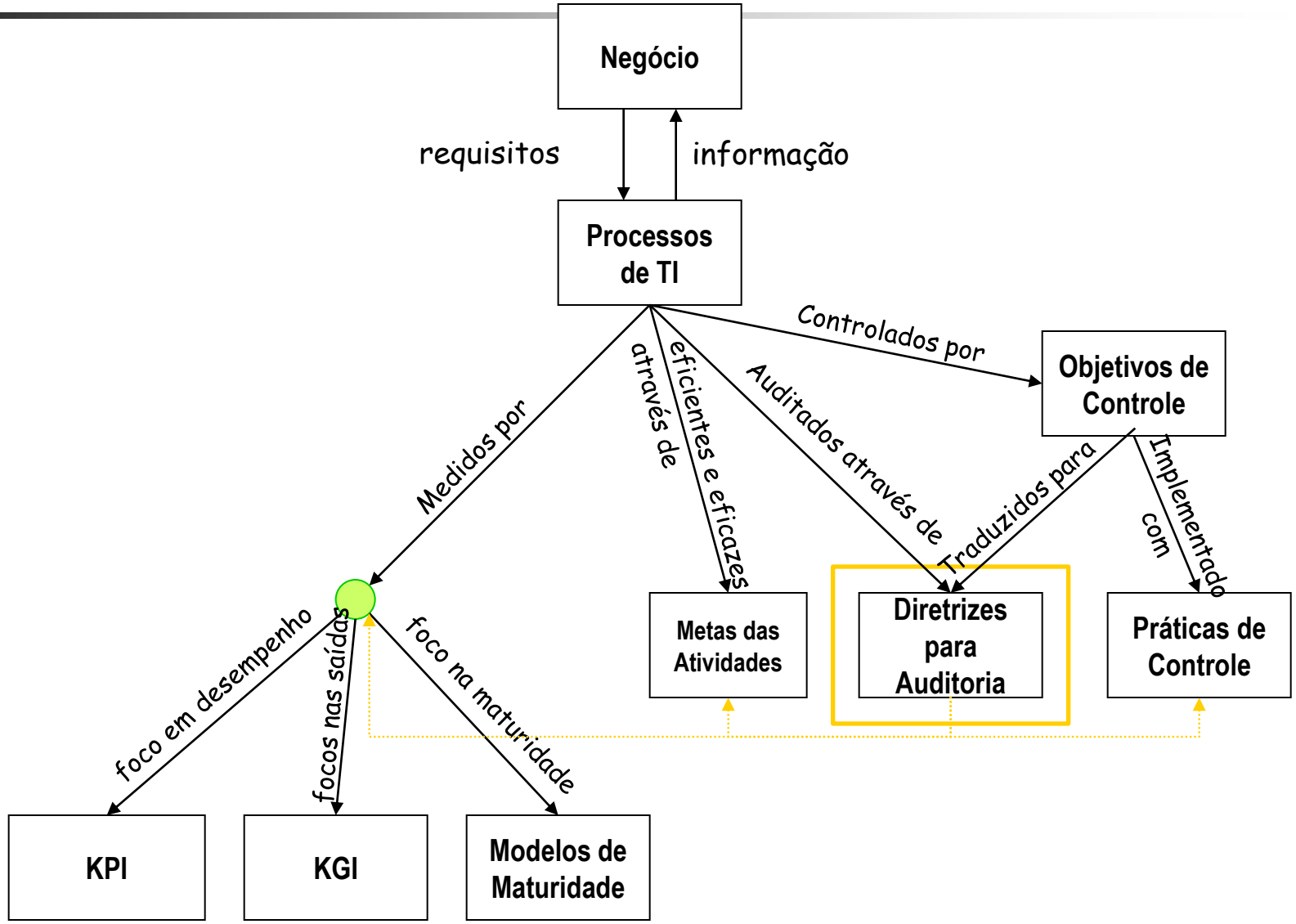
- Garantindo que o gerenciamento de risco está totalmente embutido no processo de gerenciamento, internamente e externamente, e consistentemente aplicado;
- Avaliação da performance dos riscos;
- Recomendação e comunicação dos planos de ação para correção dos riscos.

e medido por

- Percentual de objetivos críticos de TI cobertos pela avaliação de riscos;
- Percentual de riscos de TI críticos identificados com planos de ação desenvolvidos;
- Percentual de plano de ação de gerenciamento de riscos aprovados para implementação.



COBIT- Componentes Inter-relacionados



Estrutura do COBIT

- Modelos de Maturidade
  - Nível 0 (Inexistente): Processos de gestão não são aplicados;
  - Nível 1 (Inicial): Processos são esporádicos e desorganizados;
  - Nível 2 (Repetitivo): Processos seguem um padrão de regularidade;
  - Nível 3 (Definido): Processos são documentados e comunicados;
  - Nível 4 (Gerenciado): Processos são monitorados e medidos;
  - Nível 5 (Otimizado): Boas práticas são seguidas e otimizadas.

Estrutura do COBIT

- Metas e medições de desempenho
  - Indicadores-Chave de Metas (KGIs)
    - Definem as medições que informam à gerência se um processo de TI atingiu os objetivos de negócio;
  - Indicadores-Chave de Desempenho (KPIs)
    - Definem as medições que informam à gerência o quanto os processos de TI estão sendo bem executados no sentido de viabilizar o atendimento dos objetivos de negócio.

Estrutura do COBIT

- Fatores Críticos de Sucesso
  - Define as questões ou ações mais importantes para obter o controle sobre os processos de TI, estrategicamente, tecnicamente e em termos organizacionais ou procedurais.

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

- **Modelo de Maturidade:** Controle sobre o processo de TI de **Avaliar e Gerenciar Riscos de TI** com o objetivo de negócio de suportar decisões da administração através do atingimento dos objetivos de TI e fazer frente às ameaças mediante a redução da complexidade, o aumento da objetividade e a identificação de importantes fatores de decisão.
  - **0 Inexistente** A avaliação de risco para processos e decisões de negócio não ocorre. A organização não considera os impactos do negócio associados com as vulnerabilidades da segurança e com as incertezas do projeto do desenvolvimento. A gerência de risco não foi identificada como relevante para adquirir soluções de TI e entrega de serviços de TI.

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

- **1 Inicial** A organização está ciente de suas responsabilidades e obrigações legais e contratuais, mas considera os riscos de TI de uma maneira ad hoc, sem seguir processos ou políticas definidas. As avaliações informais do projeto de risco ocorrem como determinado por cada projeto. As avaliações de risco provavelmente não são identificadas especificamente dentro de um projeto planejado ou são atribuídas aos gerentes específicos envolvidos no projeto.....

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

- **2 Repetível mas Intuitivo** Há emergente compreendimento que riscos de TI são importantes e necessários serem considerados. Alguma abordagem à avaliação de risco existe, mas o processo é ainda imaturo e em desenvolvimento. A avaliação está geralmente em um alto-nível e é tipicamente aplicada somente aos projetos principais.....

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

- **3 Processo Definido** Uma ampla política de gestão de risco na organização define quando e como conduzir as avaliações de risco. A avaliação de risco segue um processo definido que está documentado e disponível a toda a equipe de funcionários treinada. As decisões para seguir o processo e para receber o treinamento são deixadas à discrição do indivíduo.....

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

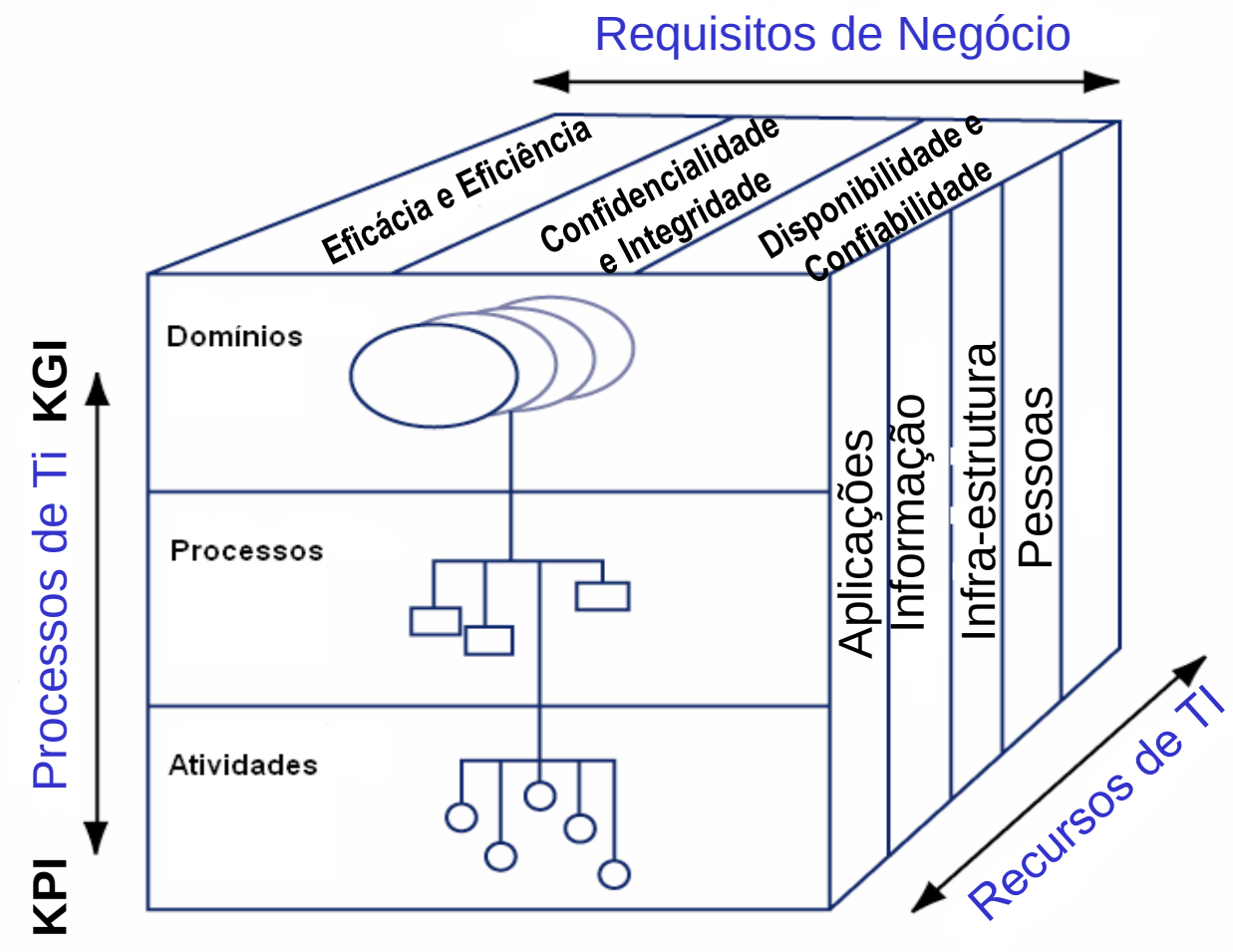
- **4 Gerenciado e Medido** A avaliação do risco é um procedimento padrão e as exceções para seguir o procedimento estão sendo observadas pela gerência de TI. É provável que a gestão de risco de TI é uma função definida da gerência com nível de responsabilidade sênior. O processo é avançado e o risco é avaliado no nível do projeto individual e também regularmente no que diz respeito a operação de TI por toda a parte.....

Diretrizes de Gerenciamento
PO9 – Avaliar e Gerenciar os Riscos de TI

- **5 Otimizado** A avaliação de risco foi desenvolvida ao estágio onde um amplo processo estruturado na organização é reforçado, seguido regularmente e bem controlado. O brainstorming e a análise de causas de risco, envolvendo os indivíduos peritos, são aplicados através da organização inteira. A captura, a análise e relato de dados da gestão de risco são altamente automatizados.....

Estrutura do Cubo COBIT

- Recursos de TI são gerenciados por Processos de TI, para atingir Metas de TI, que por sua vez estão estreitamente ligadas aos Requisitos de Negócio.



Implementando COBIT

- Documentação
  - Mapeamento dos processos de negócio
  - Definição de políticas
  - Identificação dos objetivos de controle
  - Definição de diretrizes
- Implementação
  - Divulgação
  - Conscientização
- Gestão dos processos
  - Benchmarks das práticas de controle de TI (Modelo de Maturidade – CMM)
  - Fatores Críticos de Sucesso
  - Indicadores de Objetivos
  - Indicadores de Performance

Aplicabilidade do COBIT

- Avaliação dos processos de TI
- Auditoria dos riscos operacionais de TI
- Implementação modular da Governança de TI
- Realização de *benchmarking*
- Qualificação de fornecedores de TI

Relacionamento dos Modelos de Melhores Práticas

- Nas duas últimas décadas vem surgindo e sendo elaborada uma série de modelos de melhores práticas de TI
- Alguns desses modelos são originais e outros são derivados e/ou evoluídos de outros modelos
- Exemplos:
  - CMMI, ITIL, BS 7799, ISO/IEC 27001, eSCM-SP, PMBOK, BSC, SAS-70

Estudo de Caso

Estudo de Caso:
Accor Services Brasil

Perfil da Empresa

- Accor Services- Grupo mundial de Hotelaria, Turismo e Serviços com volume de negócios de R$ 7,0 bilhões em 2004.
- No Brasil, o Grupo Accor atua fortemente no ramo de hotelaria e serviços diversificados, como os hotéis Sofitel, Mercury, Íbis, Formule 1 e Parthenon Flats, e alinha de serviços representada pelos produtos Ticket restaurante, Ticket alimentação

Histórico de TI

- Até 1999, a área de TI apresentava a seguinte situação:
  - Cada aplicação focava um único produto
  - Os sistemas eram heterogêneos e não estavam totalmente integrados
  - A arquitetura de TI não atendia à crescente necessidade de flexibilidade
  - Altos custos de manutenção dos sistemas
  - Infra-estrutura não estava totalmente alinhada com as necessidades do negócio
  - Baixo valor agregado que TI fornecia ao negócio

Reformulação de TI

- De 2000 a 2004, efetuada a implementação do ERP e CRM
- A área de Infraestrutura de TI foi transferida para IBM em um contrato de *full outsourcing* e a parte de telecomunicações com a Embratel
- As arquiteturas de TI passaram para a WEB, ao contrário do cliente/servidor
- Foi criada uma área de Segurança da Informação
- Em 2003, foi elaborado e implementado o BSC da área de TI
- A partir de 2004, ações voltadas para Governança de Ti começaram a ser pensadas e implantadas

O Programa de Governança de Ti

- O programa de desenvolveu em dois momentos.
- Em 2004, o primeiro momento consistiu nas seguintes ações:
  - Reorganização da gestão operacional de outsourcing
  - Implantação do Escritório de Projetos vinculado a diretoria de TI
  - Implantação de ferramentas para a gestão de demandas e projetos
  - Desenvolvimento da metodologia de gestão e de desenvolvimento de sistemas e processos

O Programa de Governança de Ti

- O segundo momento aconteceu em 2005, com ações tais como:
  - Criação de um modelo de governança
  - Gestão do *Portfolio* de Projetos pelo Escritório de Projetos
  - Forte capacitação dos recursos humanos em planejamento de projetos e em tecnologia

O Programa de Governança de Ti

- Como a Governança de TI evoluiu ao longo do tempo, novas ações estão sendo planejadas para 2006:
  - Administrar a TI como se fosse uma empresa
  - Implantar processos alinhados com a ITIL
  - Mudar a forma de comunicação com o negócio

Resultados alcançados até o momento

- O volume de negócio mais que duplicou nos últimos cinco anos
- O custo de TI, proporcionalmente ao resultado, caiu em mais de 30% e com melhor nível de serviço
- A satisfação do usuário aumentou em mais de 50% de 2000 a 2004
- O *backlog* diminuiu de 40% para 10%

Utilização do COBIT- Exemplos

- Banco Bradesco
  - Investimento de 1.2 bilhões no projeto “Melhorias TI” nos próximos 6 anos
- Banco Nossa Caixa
  - Em cerca de dez dias, depois de divulgado as práticas de Governança de TI, as ações da Nossa Caixa valorizaram mais de 4%, superando o Ibovespa, principal índice de preços da bolsa, no mesmo período.
- O Cobit também tem sido adotado pelas organizações de TI de grandes bancos (Itaú, Bradesco) e de grandes empresas (Grupo Votorantim, Petrobrás, Gerdau, Grupo Abril).