PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO.
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS.

ATIVIDADE EXTERNA À DISCIPLINA (AED)

RESUMO DO COBIT

BRUNO CAMARGO MANSO
JOÃO VICTOR CARDOSO DE OLIVEIRA
NIKOLLY CARDOSO DE FARIA

GOIÂNIA, GO
2020

BRUNO CAMARGO MANSO
JOÃO VICTOR CARDOSO DE OLIVEIRA
NIKOLLY CARDOSO DE FARIA

ATIVIDADE EXTERNA À DISCIPLINA (AED)
RESUMO DO COBIT

Pesquisa sobre problemas que ocorrem em empresas.
Da escolha de um processo até a solução do problema.

Orientador: Aníbal Vicente Vieira

GOIÂNIA, GO
2020

1. Introdução

A governança de TI tem um papel fundamental dentro das empresas, onde alinha a TI com os objetivos da empresa, garantindo que os recursos estejam sendo aplicados corretamente e reduzindo os riscos. A adoção de um framework de processos, como por exemplo o CobiT, pode se mostrar uma grande aliada na hora de implantar essa governança.
CobiT significa Objetivos de Controle de Informação e Tecnologia Relacionada, é um modelo de controle que garante a integridade do sistema de informação.
Neste trabalho serão apresentados aspectos desse modelo, seu histórico, objetivos, estrutura, sua aplicabilidade, e também os benefícios que sua utilização pode trazer à empresa.

2. Estudo dos processos do Modelo Cobit

2.1. CobiT - Introdução

Neste ponto falaremos um pouco sobre Cobit, sua história, seus objetivos, sua aplicação e diversas explicações resumidas a respeito do modelo e suas perspectivas.

2.1.2. Histórico do Modelo

O CobiT (Control Objectives for Information and related Technology) foi criado em 1994 pela ISACF23 a partir do seu conjunto inicial de objetivos de controle e vem evoluindo através da incorporação de padrões internacionais técnicos, profissionais, regulatórios e específicos para processos de TI. Desde então em 1998, 2000 e 2005 ele sofreu mudanças e alterações significativas, em 2007 ele sofreu apenas uma atualização incremental (versão 4.1 após a 4.0 de 2005) cujo foco foi orientado a uma maior eficácia dos objetivos de controle e dos processos de verificação e divulgação de resultados e em 2012 o cobit ganhou um novo cenário, o cobit 5.0.

2.1.3. Objetivo do Modelo

O principal objetivo das práticas do CobiT é 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. De acordo com o ITGI, neste sentido, o CobiT:

1. Estabelece relacionamentos com os requisitos do negócio.
2. Organiza as atividades de TI em um modelo de processos genérico.
3. Identifica os principais recursos de TI, nos quais deve haver mais investimento.
4. Define os objetivos de controle que devem ser considerados para a gestão.

O modelo do CobiT é genérico o bastante para representar todos os processos normalmente encontrados nas funções da TI e compreensível tanto para a operação como para os gerentes de negócios.

2.2 Estrutura do Modelo

A estrutura (framework) do CobiT foi idealizada de forma a atender às necessidades de controle da organização relacionadas à Governança de TI, tendo como principais características o foco nos requisitos de negócio, a orientação para uma abordagem de processos, a utilização extensiva de mecanismos de controle e o direcionamento para a análise das medições e indicadores de desempenho obtidos ao longo do tempo.

2.2.1. Foco no negócio

Segundo o CobiT, para fornecer a informação de que a empresa necessita para atingir as suas metas de negócio, é necessário associá-los às suas metas de TI, assim como gerenciar e controlar os recursos de TI, utilizando um conjunto estruturado de processos para garantir a entrega dos serviços de TI.

O CobiT pressupõe ainda que as informações desejadas devem obedecer a alguns requisitos de negócio, de forma que sua utilização seja proveitosa para os objetivos de negócio.

O princípio básico do Cobit em uma organização conta com Requisitos de Negócio, Recursos de TI, Processos de TI e Informações Empresariais, que são pontos que se auto relacionam e são dependentes uma das outros.

2.2.2. Orientações para processos

O CobiT fornece um modelo padrão de referência e uma linguagem comum, permitindo que todos em uma organização sejam capazes de distinguir e gerenciar atividades no âmbito da TI. Neste sentido, utilizando como matriz o ciclo tradicional de melhoria contínua (planejar, construir, executar, monitorar), Modelos Abrangentes de Governança de TI 215 o CobiT identificou 34 processos de TI e os distribuiu entre quatro domínios, que espelham os agrupamentos usuais existentes em uma organização padrão de TI:

1. Planejamento e Organização (PO).
2. Aquisição e Implementação (AI).
3. Entrega e Suporte (DS25).
4. Monitoração e Avaliação (ME26).

2.2.3. Controle através de Objetivos

Segundo o CobiT, controle é “o conjunto de políticas, procedimentos, práticas e estruturas organizacionais desenvolvidas para dar uma garantia razoável de que os objetivos de negócio serão atingidos e de que eventos indesejáveis serão prevenidos ou mesmo detectados e corrigidos”. Um objetivo de controle é um

propósito a ser atingido através da implementação de procedimentos de controle em uma atividade de TI específica.

A dinâmica de controle é bastante trivial: as informações de controle extraídas da operação de cada processo de TI são comparadas aos objetivos de controle (assim como às normas e padrões vigentes), e ações corretivas/preventivas são empreendidas para a melhoria do processo. Cada processo de TI do CobiT tem uma descrição de processo e vários objetivos de controle detalhados.
Há requisitos de controle genéricos, como:

-Definição e divulgação de metas e objetivos específicos para cada processo.
-Estabelecimento de um "dono" para o processo, com responsabilidades claras.
-Repetibilidade, visando a geração dos resultados esperados de forma consistente.
-Papéis e responsabilidades definidos sem ambiguidades.
-Definição e divulgação das políticas, procedimentos e planos relativos ao processo.
-Desempenho do processo medido em relação às respectivas metas.

Podem também existir controles específicos vinculados a aplicações, integrados aos processos de negócio que os suportam através de procedimentos relacionados a:

-Autorização e criação de dados.
-Entrada de dados.
-Processamento de dados.
-Saída de dados.
-Interfaces.

2.2.4. Direcionamento para medições

Para saber o nível de profundidade que deve ser adotado pelos mecanismos de controle e medições de desempenho deve-se, primeiro, definir o que deve ser medido, como e onde obter os dados e em que perspectiva os resultados devem ser agregados. As empresas devem medir a situação atual e monitorar essas ações de forma sistemática. Para decidir qual é o ponto certo deve-se analisar a relação custo-benefício do controle.

A abordagem do CobiT para questões como essas compreende:

Modelos de Maturidade: é baseado em níveis, através do qual uma organização poderá ser avaliada como:

- Nível 0 (Inexistente): processos de gestão não são aplicados;
- Nível 1 (Inicial/Ad Hoc): processos são esporádicos e desorganizados, com abordagens de gestão aplicadas caso a caso.
- Nível 2 (Repetitivo mas Intuitivo): processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
- Nível 3 (Definido): processos são padronizados, documentados e comunicados.
- Nível 4 (Gerenciado e Mensurável): processos são monitorados e medidos, e ações são tomadas quando os resultados não são efetivos.
- Nível 5 (Otimizado): boas práticas são seguidas e automatizadas.

Através destes modelos de maturidade, a gerência tem condições de:

- Mapear a situação atual da organização.
- Comparar com a situação das melhores organizações no segmento (benchmarking).
- Comparar com padrões internacionais.
- Estabelecer e monitorar passo a passo as melhorias dos processos rumo à estratégia da organização.

Metas e Medições de Desempenho: demonstram o que o negócio espera da TI, o que o processo de TI precisa entregar para suportar os objetivos da TI e o que precisa acontecer dentro do processo para que o desempenho requerido seja atingido. O CobiT usa dois tipos de indicadores:

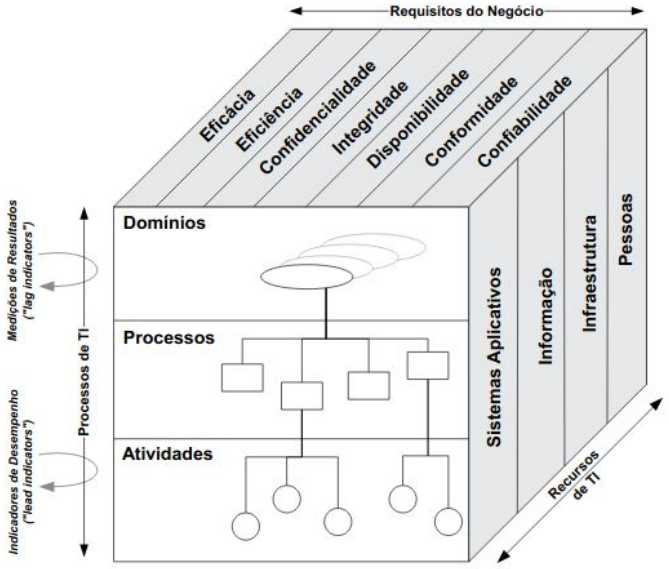
- Medições de Resultados (Outcome Measures) definem as medições que informam à gerência se um processo de TI atingiu os objetivos de negócio.
- Indicadores de Desempenho (Performance Indicators) definem as medições que informam à gerência o quanto os processos de TI estão sendo bem executados no sentido de viabilizar o atendimento dos objetivos de negócio.

Analogamente, as medições de resultados em um determinado nível podem se tornar indicadores de desempenho para o nível superior. Por exemplo, a quantidade de incidentes causados por acesso não autorizado pode ser um indicador de desempenho ligado à meta de TI “assegurar que os serviços de TI resistam e possam se recuperar de ataques”.

2.2.5. Visão Integrada do Modelo

CobiT pode então ser definido pelo seu framework, isso inclui os Recursos de TI que são gerenciados pelos processos de TI com objetivo de alcançar as metas de TI estabelecidas pelos Requisitos de Negócios

A seguir na figura abaixo, retirada do livro “Implantando a Governança de TI”, temos uma representação de uma visão adequadamente integrada, o Cubo de CobiT:



2.2.6. Conteúdo dos processos de TI

Os processos de TI são integrantes do núcleo do CobiT. Cada um dos 34 processos de TI são descritos através dos seus componentes, que relacionam-se entre si.

É representado em forma de cascata, mostrando o mapeamento do processo seguindo critérios, o sumário de metas de TI juntamente com as atividades mais importante e o sumário das métricas-chave para o processo.

Segundo Aragon (2012), os objetivos de controle são detalhados juntamente com suas atividades. Existem diretrizes para gerenciamento que definem as entradas e saídas, a matriz de responsabilidade, as metas de cada atividade e o cruzamento de informações entre o desempenho e as metas.

Um modelo de maturidade é exigido para que seja então feito o devido benchmark entre o criado e o exigido.

2.2.7. Produtos CobitT complementares

Além do documento principal do Cobit e seu framework, diretrizes e objetivos de controle, existem produtos que são mais específicos para cada regra de negócio, tais como: *O Board Briefing IT Governance; Building the Business Case for CobiT*

and Val IT - Executive Briefing; Information Security Governance: Guidance for Boards of Directors and Executive Management; Implementing and Continually Improving IT Governance; CobiT Online; Cobit Training; CobiT Quickstart; Cobit Security Baseline; CobiT mappings; CobiT user Guide for Service Managers; Cobit and Application Control: a management guide; CobiT Control Practices; IT Assurance Guide - using CobiT; IT Control Objectives for Sarbanes-Oxley; Val IT.

2.3 Aplicabilidade do Modelo

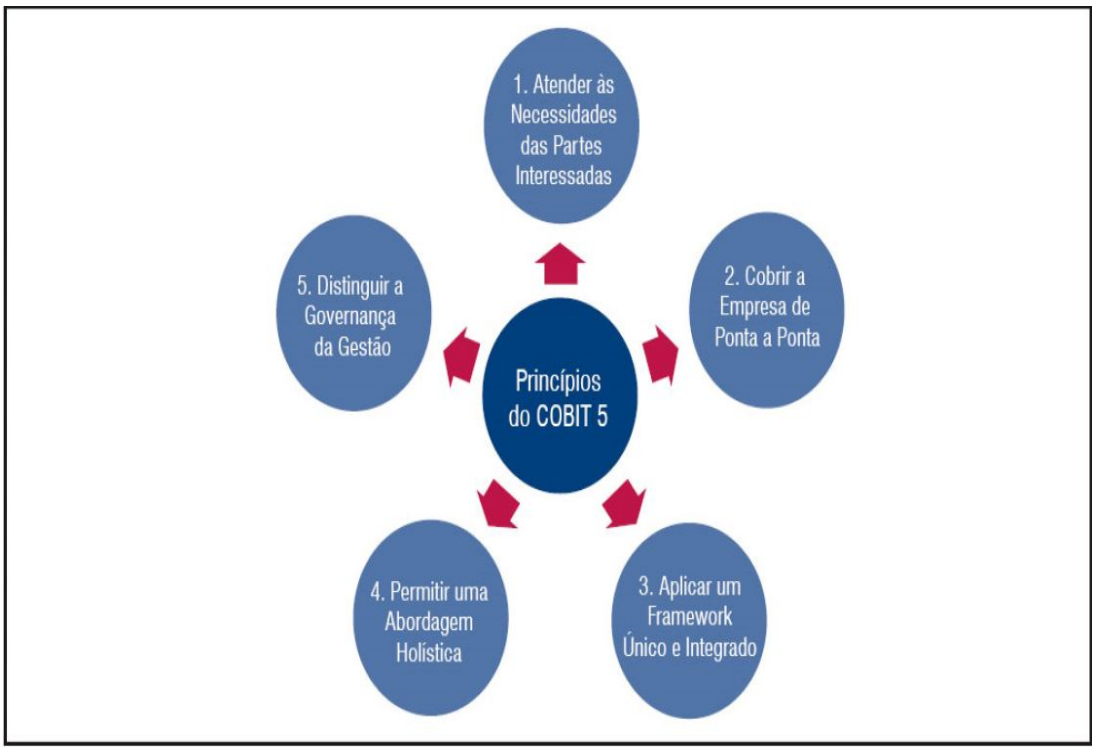
Estando tudo alinhado com os requisitos de alto nível e com a boa convivência com outros padrões existentes no mercado, o CobiT cobre todas as atividades de TI, porém com foco em o que deve ser atingido. É usado, então em um nível estratégico dentro das empresas, delineando estruturas de controle e gestão que abrange a organização por completo.

Aragon (2012), em seu livro Implantando a Governança de TI, destaca que não se deve perder oportunidades de aplicação dessa ferramenta quando há necessidade de avaliação dos processos de TI, auditoria de riscos operacionais, implementação modular de Governança, realização de *benchmarking* ou ainda na qualificação de fornecedores de TI.

O CobiT então pode abranger a maioria das organizações, pequenas ou grandes, se ao menos esteja consistente com os objetivos de negócios e estratégias impostas pela TI. E dentro de uma organização, o foco da implementação do CobiT pode ser tanto sua gestão executiva, como a gestão de negócios, de TI e os auditores.

2.3.1. Princípios do modelo Cobit

É necessário que um conjunto de princípios para melhor implementação de padrões e boas práticas e que consiga ser modularmente adaptado de forma que seja utilizado de forma gradual conforme a necessidade de melhoria, determinado pelo planejamento estratégico.



1º Princípio: Atender às Necessidades das Partes Interessadas - Organizações existem para criar valor para suas Partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. Como cada organização tem objetivos diferentes, o COBIT 5 pode ser personalizado de forma a adequá-lo ao seu próprio contexto por meio da cascata de objetivos.

2º Princípio: Cobrir a Organização de Ponta a Ponta - O COBIT 5 é capaz de:
Cobre todas as funções e processos corporativos; O COBIT 5 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo na organização por completo.
Também inclui tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

3º Princípio: Aplicar um Modelo Único Integrado - O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como o um modelo unificado para a governança e gestão de TI da organização, não necessitando ir em busca de novos padrões e modelos por ter tudo em um único lugar.

4º Princípio: Permitir uma Abordagem Holística - O COBIT 5 define um conjunto de

habilitadores(vem de habilidade que pode ser qualquer coisa que venha a ajudar a atingir objetivos) para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. O modelo do COBIT 5 define sete categorias de habilitadores:

1. Princípios, Políticas e Modelos
2. Processos
3. Estruturas Organizacionais
4. Cultura, Ética e Comportamento
5. Informação
6. Serviços, Infraestrutura e Aplicativos
7. Pessoas, Habilidades e Competências

5º Princípio: Distinguir a Governança da Gestão – O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciadas e servem a propósitos diferentes dentro da organização.

2.4. Benefícios do Modelo

A estrutura do CobiT favorece muito o entendimento dos processos de TI e por consequência, fornece um excelente guia para a sua implementação ou melhoria nas organizações, assim como, para a avaliação da maturidade atual dos processos existentes. Alguns benefícios que a utilização sistemática do CobiT poderá trazer, são:

- Responsabilidades e protocolos de comunicação bastante claros;
- Visão clara acerca da situação atual dos processos de TI e de seus pontos de vulnerabilidade.
- Redução da exposição a riscos;
- Maior solidez e assertividade no planejamento encadeado das ações de melhoria;
- Alta visibilidade acerca do impacto dos esforços de melhoria nos processos de TI e dos seus reflexos nos processos de negócio;
- Redução dos custos operacionais e de propriedade do acervo de TI;

- Melhoria da imagem perante os clientes.

Conclui-se que uma organização que utiliza o CobiT poderá estabelecer bases mais sólidas para um melhor retorno sobre os investimentos em TI.

3. Bibliografia

ARAGON, Aguinaldo; ABREU, Vladimir Ferraz. **Implantando a Governança de TI.** Da Estratégia à Gestão dos Processos e Serviços. 3a Edição. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2012.

ISACA FRAMEWORK. **COBIT 5.** Modelo Corporativo para Governança e Gestão de TI da Organização. 5a Edição. USA:2012.