

Engenharia de Controle e Automação – 9º Período
Disciplina: Aspectos de Segurança em Automação
Professor: José Maurício S. Pinheiro

AULA 2: Normas e Guias de Referência para Governança

As redes de automação industrial são estabelecidas para elevar a produtividade dos processos. Com a evolução das tecnologias de comunicação e as novas demandas de mercado, observa-se a convergência das redes de Tecnologia da Informação (TI) com as de Tecnologia da Automação (TA). Neste contexto, torna-se necessário aperfeiçoar o modelo de gestão da empresa, bem como a maneira na qual a gestão está sendo realizada e fiscalizada.

1. Modelos e Ferramentas de Governança

De acordo com o IBGC (Instituto Brasileiro de Governança Corporativa) a Governança Corporativa é “o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, administração, diretoria e órgãos de controle. As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade”.

Para se garantir um bom uso da Governança Corporativa como um todo, foram criados inúmeros modelos (*frameworks*) e ferramentas, dentre eles se destacam:

1.1. BSC

O BSC (*Balanced Scorecard*) é uma ferramenta eficiente para se elaborar a “Estratégia Corporativa” de uma empresa. Para possibilitar uma boa Governança de TI é imprescindível que a estratégia de TI da empresa esteja perfeitamente alinhada com a Estratégia Corporativa como um todo. Com o uso do BSC visualiza-se o quadro geral da empresa por meio de quatro perspectivas: financeira; cliente; processos internos; e aprendizado / crescimento. Com base nelas é gerado um mapa estratégico do qual são traduzidas a missão e a visão da empresa, além de indicadores e medições de desempenho vitais para uma boa gestão (Figura 1). As seguintes perguntas devem ser respondidas:

- Onde queremos ir agora? – Extração da visão da empresa e dos objetivos do negócio.
- Onde estamos agora? – Avaliação da situação atual da empresa (Inclui desenho dos processos e definição dos indicadores).

- Como chegaremos lá? – Definição da Estratégia Corporativa com base nas informações anteriores. (Inclui nova definição de indicadores e processos)
- Como saberemos se chegamos? – Medições de resultados com base nos indicadores previamente definidos.



Figura 1 - Fluxo BSC

1.2. COBIT

COBIT é o acrônimo de *Control Objectives for Information and Related Technology* ou em uma tradução direta “Controle de Objetivos para Informação e Tecnologia Relacionada”. Trata-se de uma ferramenta para auxiliar o gerenciamento e controle das ações de TI nas organizações com vistas a garantir o alinhamento entre TI e negócios.

O objetivo do modelo COBIT é pesquisar, desenvolver e publicar um conjunto atualizado de padrões internacionais e de melhores práticas referentes ao uso corporativo de TI para os gerentes e auditores de tecnologia. Desenvolvido e difundido pelo ISACA (*Information System Audit and Control*) e pelo *IT Governance Institute*.

O modelo COBIT segue diretrizes internacionais e descreve as melhores práticas para gerenciamento dos recursos de tecnologia da informação. O objetivo final é garantir o alinhamento estratégico da organização.

1.2.1. Domínios do COBIT

O COBIT estabelece métodos formalizados para orientar as decisões tecnológicas das organizações, envolvendo qualidade, maturidade, planejamento e segurança. Encontra-se organizado em quatro domínios que são detalhados em processos e os respectivos processos são detalhados em atividades:

- Planejamento e organização;
- Aquisição e implementação;
- Entrega e suporte;
- Controle e avaliação.

A Figura 2 ilustra a estrutura do COBIT com os quatro domínios:

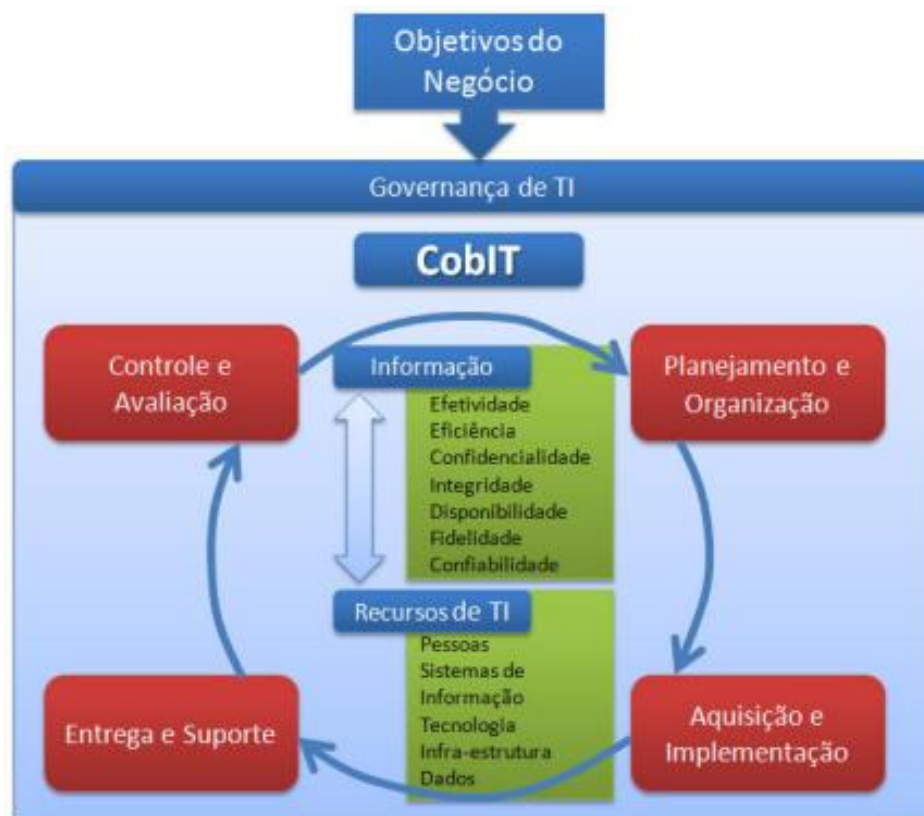


Figura 2 - Governança de TI e estrutura COBIT

1.2.2. Planejamento e Organização

Esse domínio possui onze processos de controle que visam garantir o alinhamento estratégico entre a área de negócios e a área de TI, a saber:

- Define o plano estratégico de TI;
- Define a arquitetura da informação;
- Determina a direção tecnológica;
- Define a organização de TI e seus relacionamentos;

- Gerencia os investimentos em TI;
- Gerencia a comunicação das direções de TI;
- Gerencia os recursos humanos da área de TI;
- Assegura o alinhamento de TI com os requerimentos externos;
- Avalia os riscos;
- Gerencia os projetos;
- Gerencia a qualidade.

1.2.3. Aquisição e Implementação

Possui seis processos de controle cujo objetivo é orientar as práticas de atualização tecnológica garantindo a efetividade dos recursos:

- Identifica as soluções de automação;
- Adquire e mantém os softwares;
- Adquire e mantém a infraestrutura tecnológica;
- Desenvolve e mantém os procedimentos;
- Instala e certifica softwares;
- Gerencia as mudanças;

1.2.4. Entrega e Suporte

Possui treze processos descritos, trata da “logística” de produtos e serviços da área de informática em relação aos seus usuários:

- Define e mantém os acordos de serviços;
- Gerencia os serviços de terceiros;
- Gerencia o desempenho e capacidade do ambiente;
- Assegura a continuidade dos serviços;
- Assegura a segurança dos serviços;
- Identifica e aloca custos;
- Treina os usuários;
- Assiste e aconselha os usuários;
- Gerencia a configuração;
- Gerencia os problemas e incidentes;
- Gerencia os dados;
- Gerencia a infraestrutura;
- Gerencia as operações.

1.2.5. Controle e Avaliação

São descritos quatro processos para este domínio onde o foco principal é acompanhar o desempenho de todas as ações de TI, este domínio pode ser considerado o orientador das ações de auditoria do todo o sistema COBIT:

- Monitora os processos;
- Analisa a adequação dos controles internos;
- Provê auditorias independentes;
- Provê segurança independente.

1.3. CMMI e MPS.BR

O CMMI (*Capability Maturity Model Integration*) é um modelo de referência que contém práticas necessárias à maturidade ou capacidade dos processos. O CMU/SEI (2010) define o CMMI como “um modelo de melhoria de processo que fornece às organizações os elementos essenciais para obtenção de processos eficazes e melhoria no desempenho”. O CMMI procura estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas.

O MPS.BR é um modelo de maturidade de processos relacionados com o desenvolvimento de software sendo na realidade a adequação do CMMI-DEV para o mercado brasileiro. Isto foi necessário, pois o mercado nacional apresenta um nível de granularidade maior do que a média mundial e consequentemente evolui de maneira mais gradual. Assim, os cinco níveis de maturidade do CMMI-DEV foram substituídos por sete níveis no MPS.BR (Figura 3).

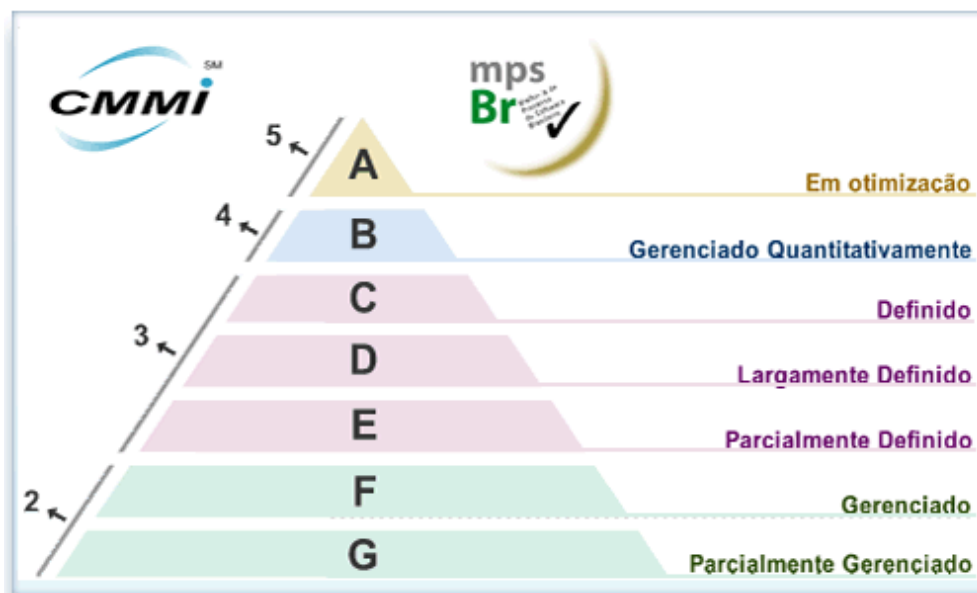


Figura 3 - CMMI – MPS.Br

1.1.ISO/IEC 38500

ISO/IEC 38500 (Governança corporativa de tecnologia da informação) é um padrão internacional para a governança corporativa de TI. Esta norma estabelece seis princípios orientadores para diretores de organizações sobre o uso eficaz, eficiente e aceitável da TI dentro de suas organizações: Responsabilidade; Estratégia; Aquisição; Desempenho; Conformidade; e Comportamento humano (Figura 4).

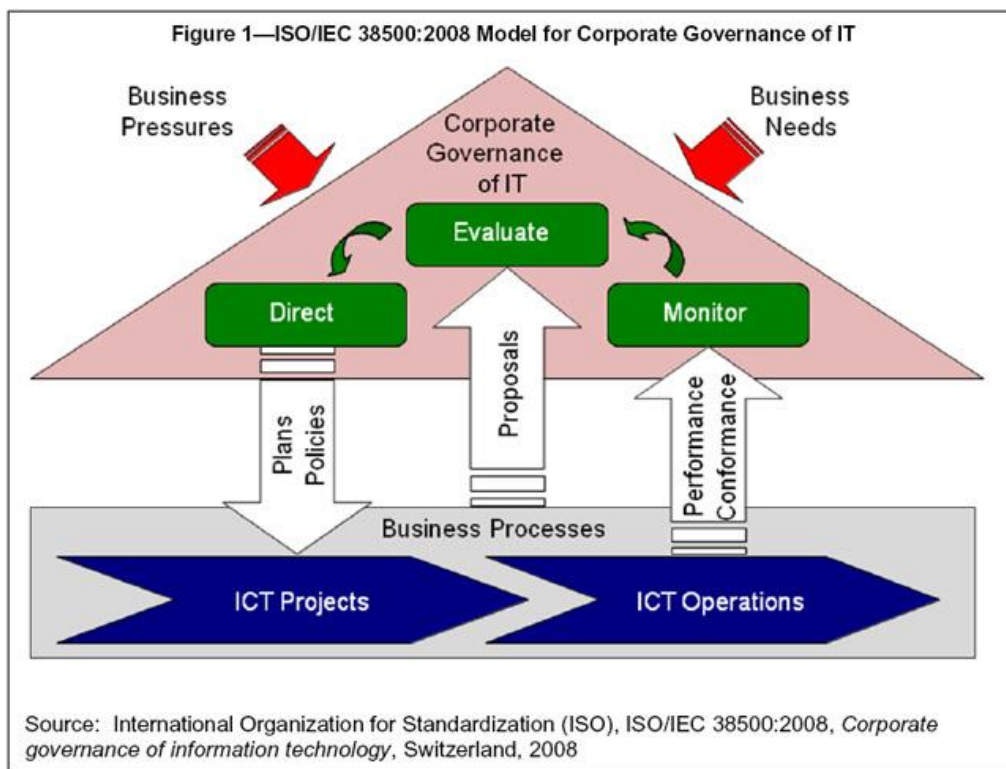


Figura 4 - ISO/IEC 38500

1.4. ITIL

O ITIL, cuja sigla significa *IT Information Infrastructure Library*, é uma biblioteca criada pelo governo britânico nos anos 1980, composta por um conjunto de recomendações e melhores práticas para operações e gerenciamento de serviços de TI, buscando proporcionar uma abordagem efetiva e eficiente no uso de sistemas de informação. Tem como objetivo principal a operação e a gestão da infraestrutura de TI incluindo aspectos de fornecimento e manutenção dos serviços de TI. O comitê gestor concluiu que, independentemente do tamanho da empresa, os custos de TI precisavam ser reduzidos e a qualidade do serviço prestado por estas áreas tinha de ser melhorado e, desta forma, surgiu a metodologia ITIL.

O ITIL é um modelo aberto, ou seja, qualquer empresa pode usar livremente a sua biblioteca (ou parte dela), o que tem contribuído para o aumento exponencial da utilização de seus processos. O foco da metodologia é mostrar “o que fazer”, e não “como fazer”, dando ênfase aos objetivos, atividades, entradas e saídas de informações, etc., fazendo com que possa ser incorporada à praticamente qualquer organização.

Atualmente as normas ITIL estão documentadas em aproximadamente quarenta livros, onde os principais processos e as recomendações das melhores práticas de TI estão descritas permitindo assim, um funcionamento eficiente e efetivo de todos os serviços de TI de uma empresa. A organização desta biblioteca se dá através de disciplinas que são subdivididas em processos:

- **A Perspectiva de Negócios** – define procedimentos para avaliar o alinhamento estratégico entre TI e Negócio;
- **Gerenciamento de Aplicações** – define procedimentos para monitorar o desenvolvimento, implantação e manutenção de aplicações na organização;
- **Entrega de Serviços** – define procedimentos para fazer com que as solicitações do usuário cheguem até eles com o nível de serviço desejado;
- **Suporte a Serviços** – define procedimentos para monitorar o nível de apoio à grade de serviços de TI;
- **Gerenciamento de Infraestrutura** – define procedimentos para acompanhar a evolução da infraestrutura de TI da organização.

As disciplinas de “Suporte a Serviços” e “Entrega de Serviços” formam a pedra fundamental do modelo ITIL (Figura 5) são:

1.4.1. Suporte a Serviços

- **Service Desk** – não representa uma disciplina, mas sim uma função que é responsável por acompanhar em toda a organização a satisfação do usuário;
- **Gerenciamento de Incidentes** – visa definir práticas que deem maior celeridade na resolução de contingências minimizando o impacto nos negócios;
- **Gerenciamento de Problemas** – descreve mecanismos para eliminar a reincidência de problemas, de forma proativa;
- **Gerenciamento de Mudanças** – descreve requisitos para monitorar mudanças tecnológicas garantindo uma transição segura e eficiente;
- **Gerenciamento de Atualizações e Versões** – apresenta ferramentas para controlar a disponibilidade de versões e novas aplicações para o usuário;
- **Gerenciamento da Configuração** – descrição de requisitos para padronização de configurações do ambiente computacional.

1.4.2. Entrega de Serviços:

- **Gerenciamento de Nível de Serviço** – cuida de garantir o exato atendimento dos requisitos do serviço solicitados pelo usuário;
- **Gerenciamento da Viabilidade** – corresponde aos mecanismos que permitem avaliar a viabilidade e disponibilidade da infraestrutura de TI para atender aos requisitos do usuário;
- **Gerenciamento Financeiro** – visa definir prática para administrar os recursos financeiros da organização destinados à TI;
- **Gerenciamento da Continuidade** – visa definir mecanismos que garantam a continuidade dos serviços aos usuários e clientes mesmo em situações de crise;

- **Gerenciamento da Capacidade** – descreve procedimentos para monitorar a capacidade de prover serviços ao usuário como padrão de qualidade demandada.

A partir das referências do modelo ITIL, podemos verificar quais instâncias da gestão tecnológica permitem a manutenção de um padrão elevado nos níveis de serviço de TI.

Este modelo, assim como o COBIT, procura criar um protocolo internacional para uniformização da gestão da TI, oferecendo diretrizes gerais a serem abordadas por qualquer organização de qualquer porte. Uma vez que os modelos descrevem o que fazer e não como fazer, caberá a cada organização implementar os recursos de controle de acordo com suas necessidades especiais.

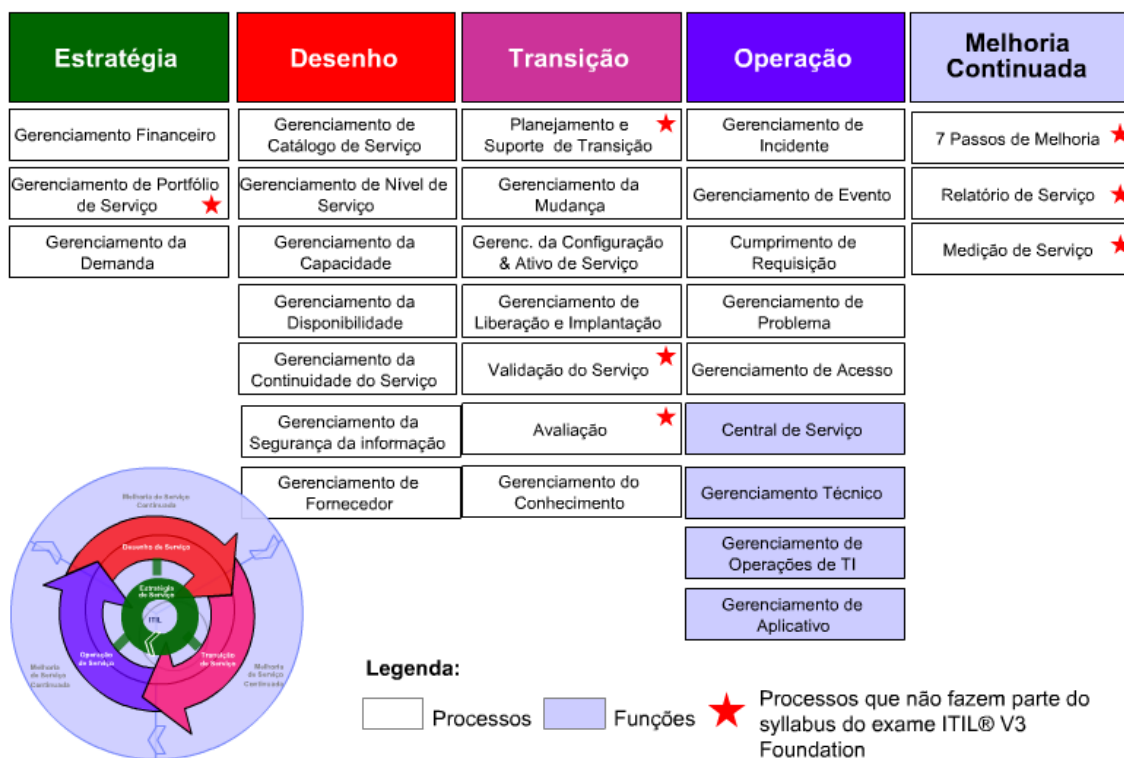


Figura 5 - Framework ITIL

1.5. PMBOK

O *Project Management Body of Knowledge* (PMBOK) é um conjunto de práticas em gerenciamento de projetos publicado pelo *Project Management Institute* (PMI) e constitui uma base de conhecimento em gerenciamento de projetos. Estas práticas são compiladas na forma de um guia, chamado de o Guia PMBOK. O Guia PMBOK baseia-se em processos e subprocessos para descrever de forma organizada as atividades a serem realizadas durante um projeto (Figura 6).

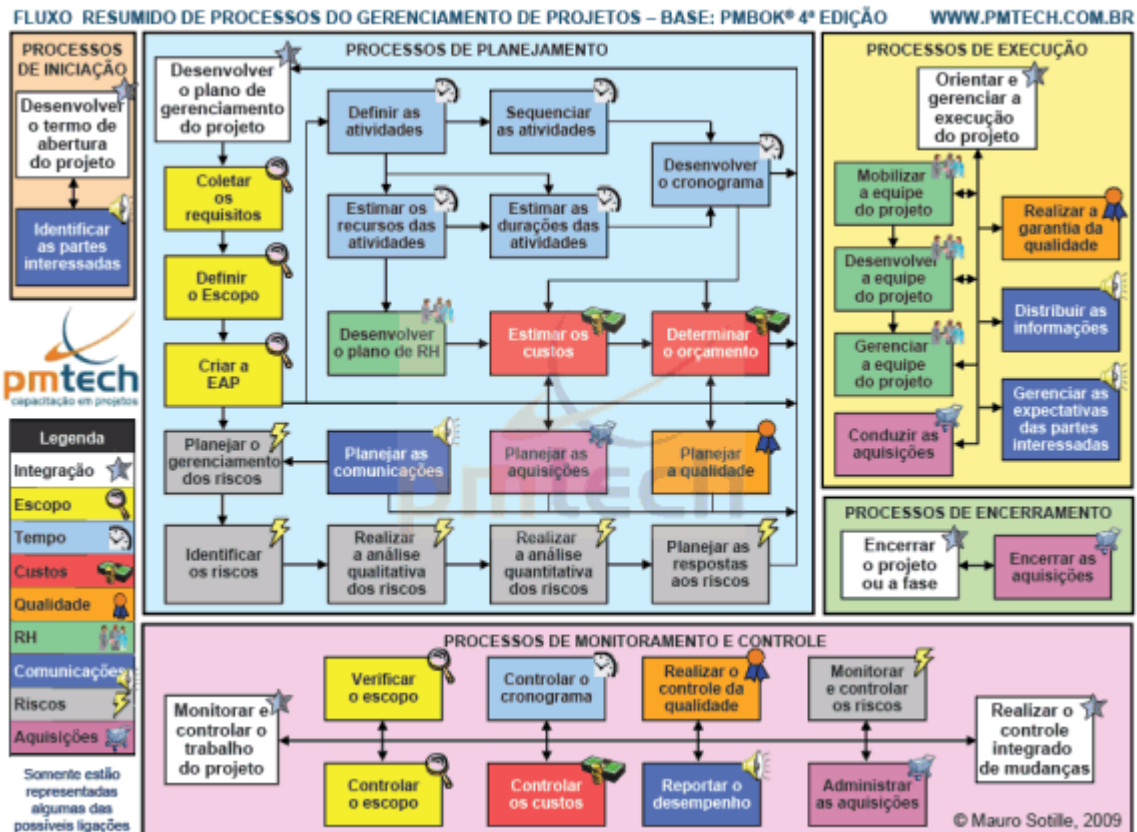


Figura 6 - Fluxo resumido PMBOK

Em resumo, escopo, tempo, custos e qualidade são os principais determinantes para o objetivo de um projeto: entregar um resultado de acordo com o escopo, no prazo e no custo definidos, com qualidade adequada (o que, quando, quanto e como). Recursos humanos e aquisições são os insumos para produzir o trabalho do projeto. Comunicações, partes interessadas e riscos devem ser continuamente tratados para manter as expectativas e as incertezas sob controle, assim como o projeto no rumo certo. E Integração abrange a orquestração de todos estes aspectos.

1.1. SIX SIGMA

O Six Sigma tem como principal finalidade atingir um elevado nível de desempenho, confiabilidade e valor para o cliente. É utilizada em todo o mundo como um dos principais temas de TQM (*Total Quality Management*). Foi desenvolvido por Bill Smith, da Motorola, em 1986, e concebido como uma forma de medir defeitos e melhorar a qualidade global. Basicamente determina uma taxa mínima de 3,4 defeitos por milhão de oportunidades, o equivalente a um padrão de qualidade de 99,9997%. Utiliza-se a metodologia DMAIC (Definir; Medir; Analisar; Melhorar; Controlar), conforme a Figura 7:

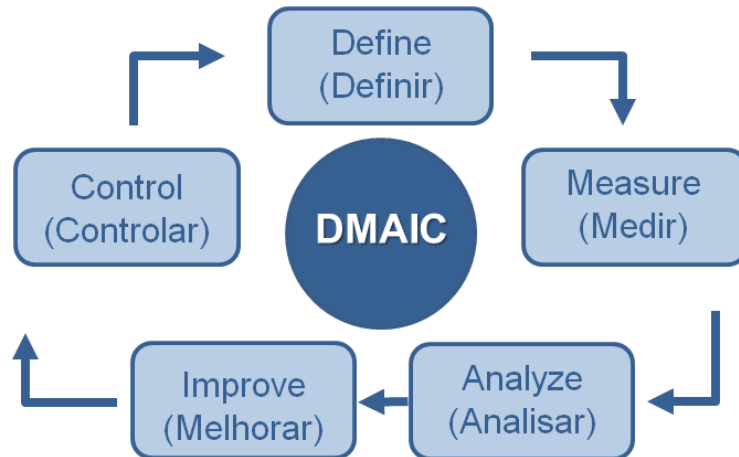


Figura 7 - Metodologia DMAIC – SIX SIGMA

1.2. TOGAF

O TOGAF (*The Open Group Architecture Framework*) é um framework que permite criar, avaliar e construir a arquitetura certa para a organização. Ele é baseado no *Architecture Development Method* (ADM), um método para o desenvolvimento de uma arquitetura de TI que atenda às necessidades da empresa e do negócio. O TOGAF é projetado para suportar ao menos quatro arquiteturas: Arquitetura de Negócio; Arquitetura de Dados; Arquitetura de Aplicações; e Arquitetura de Tecnologia (Figura 8).

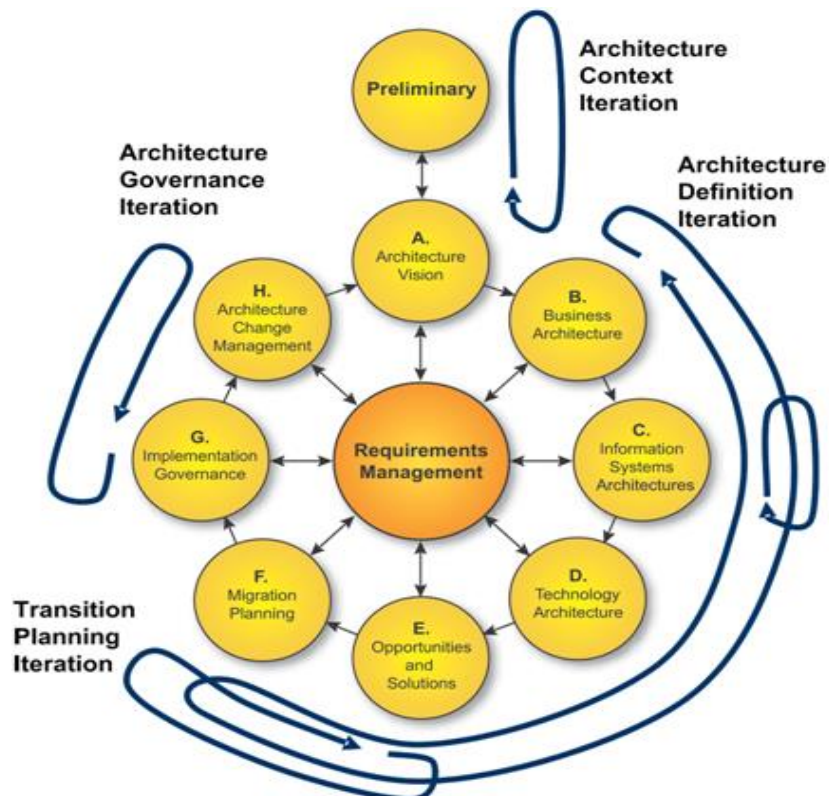


Figura 8 - Fluxo TOGAF

1.3. Val IT

O Val IT (*Value of Information Technology*) foi criado com o objetivo de ajudar os gestores a avaliar, selecionar e medir o retorno de seus investimentos (ROI) em TI. A exigência por ambientes de TI cada vez mais complexos e que ficam obsoletos mais rapidamente, faz com que a substituição de hardware e software aumente significativamente. Desenhado especificamente como um complemento ao modelo COBIT, ambos formam um ciclo completo de Governança de TI (Figura 9).

O Val IT está dividido em três domínios: Governança de Valor (VG); Gerenciamento de Portfólio (PM); e Gerenciamento de Investimento (IM).

Tem como principais objetivos:

- Ajudar a gerência a assegurar que as organizações obtenham o máximo de retorno dos investimentos habilitados por TI a um custo razoável e com um nível de risco conhecido e aceito.
- Prover diretrizes, processos e práticas de apoio para ajudar os conselhos, diretorias, equipes de gerência executivas e outros líderes da empresa no entendimento e desempenho dos seus respectivos papéis, em relação aos investimentos habilitados por TI.

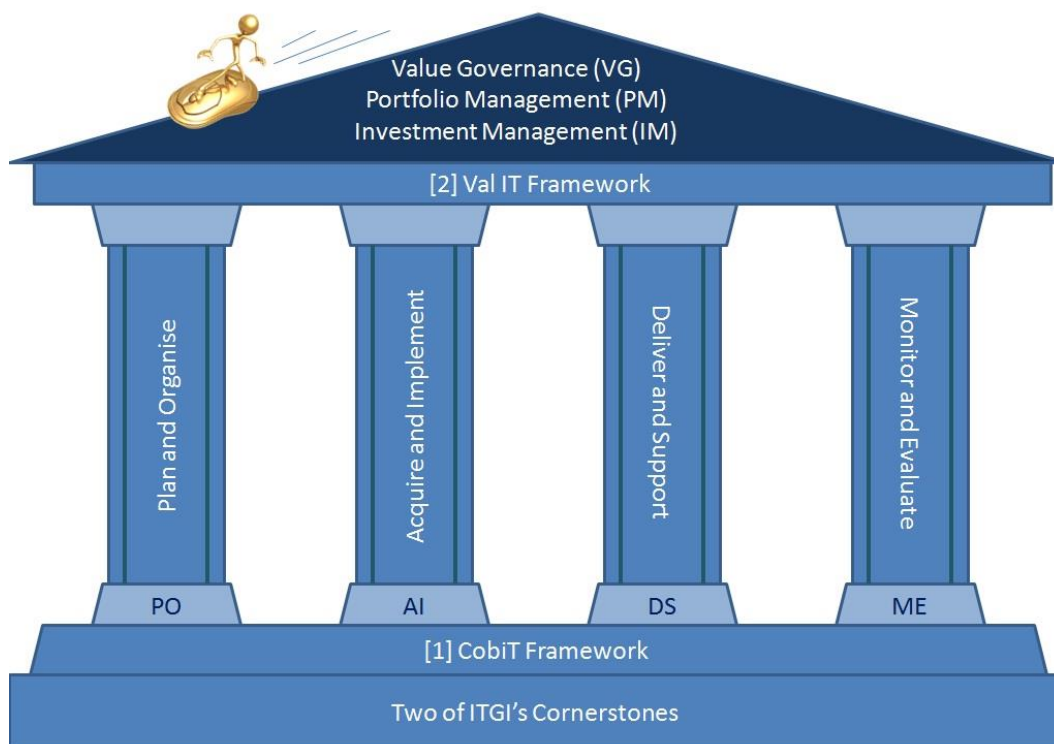


Figura 9 - Val IT