MBA em Gestão de Tecnologia da Informação

Governança em TI

Prof. Msc. Lincoln Herbert Teixeira
lincolnherbert@gmail.com

2011

Sumário

Definições de Gestão de TI

O que é Gestão?

Gestão é sinônimo de Administração, Gerir, assim como administrar, tem a ver com todo o controle e ações propostas envolvendo um conjunto que pode envolver pessoas, empresa, produtos, serviços, clientes. Gerir é conseguir controlar com eficiência, ou busca-se isso.

O termo TI (**Tecnologia da Informação**) serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. A TI está fundamentada nos seguintes componentes (Rezende, 2000):

Hardware e seus dispositivos periféricos

Software e seus recursos;

Sistemas de telecomunicações;

Gestão de dados e informações.

A Tecnologia da Informação (TI) é o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, e a maneira como esses recursos estão organizados num sistema capaz de executar um conjunto de tarefas". A TI não se restringe a equipamentos (hardware), programas (software) e comunicação de dados. Existem tecnologias relativas ao planejamento de informática, ao desenvolvimento de sistemas, ao suporte ao software, aos processos de produção e operação, ao suporte de hardware, ela também cuida de áreas como planejamento, desenvolvimento de sistemas, suporte ao software e hardware e processos de produção e operação.

O Gestor de TI é o profissional responsável pela implementação e pelo gerenciamento dos sistemas informatizados nas empresas. É de sua alçada avaliar os sistemas de informação, segurança e bancos de dados, implementar sistemas de automação no gerenciamento de informação nas instituições e determinar estratégias de utilização da informática para garantir o melhor desempenho de cada um dos setores da companhia.

O que é governança de TI?

Esta é uma questão que muitos CIOs estão fazendo. Isto ocorre devido à diversidade de ferramentas e conceitos que são "despejados" no mercado, gerando dúvidas e definições incorretas sobre o tema.

Os grandes equívocos que ocorrem frequentemente são de definição, onde se conceitua a Governança de TI (GTI) como um painel de indicadores, ou como um processo de gestão de portfólio dos projetos estratégicos.

Existem algumas frentes defensoras do conceito de que com a implementação de alguns processos baseados em apenas uma das melhores práticas (como Balanced Scoredcards (BSC), CobiT, ou ITIL) por si só, garantem a Governança, entretanto este conceito está incorreto.

A premissa mais importante da Governança de TI é o alinhamento entre as diretrizes e objetivos estratégicas da organização com as ações de TI. A definição do ilustre professor da FGV Sr. João R. Peres demonstra este conceito de forma abrangente, atribuindo os papéis e as responsabilidades conforme abaixo:

> "Governança de TI é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios."

Está definição deixa clara a importância da Governança de TI em organizações que almejam atender a crescente demanda por aumento de qualidade de produtos e processos, a alta competitividade do mercado globalizado e a busca por menores custos e maiores lucros.

Outra definição que se encaixa em Governança de TI é de considerá-la como "a Gestão da Gestão", demonstrando seu papel principal que é de auxiliar o CIO (Governante de TI) a avaliar os rumos a serem tomados para o alcance dos objetivos da organização, onde um direcionamento errado pode levar a empresa ao fracasso em pouco tempo.

Casos de sucesso de um programa de Governança aplicados a uma organização não dão a garantia do mesmo sucesso à outra. Estes casos são muito instrutivos e importantes para auxiliar nos caminhos da elaboração de um programa próprio.

A implementação efetiva da Governança de TI só é possível com o desenvolvimento de um framework (modelo) organizacional específico. Para tanto, devem ser utilizadas, em conjunto, as melhores práticas existentes como o BSC, PMBok, CobiT, ITIL, CMMI e ISO 17.799, de onde devem ser extraídos os pontos que atinjam os objetivos do programa de Governança. Além disso, é imprescindível levar em conta os aspectos culturais e estruturais da empresa, devido à mudança dos

paradigmas existentes.

O grande desafio do Governante de TI é o de transformar os processos em “engrenagens” que funcionem de forma sincronizada a ponto de demonstrar que a TI não é apenas uma área de suporte ao negócio e sim parte fundamental da estratégia das organizações.

Governança de TI, para que existe ?

Governança de TI é "um braço" da Governança Corporativa, e para entender o que é Governança de TI vamos primeiro entender o que é Governança Corporativa. Segundo o IBGC (Instituto Brasileiro de Governança Corporativa):

> *"é o sistema pelo qual as sociedades(empresas) são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/cotistas, conselho e administração, diretoria, auditoria independente e conselho fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade."*

A necessidade de se ter uma política de Governança se deu, pois ao longo do tempo a complexidade das organizações, concorrência e partes interessadas, os famosos stakeholders aumentaram muito. A abertura de capital, ou seja, o fato das empresas negociarem suas ações na bolsa contribuiu muito para a necessidade de uma maior transparência, para que os atuais acionistas saibam como vai seu investimento e para que novos acionistas sejam atraídos (saímos de um contexto onde a empresa era administrada pelos "sócios" para um cenário onde os acionistas nunca colocaram o pé dentro da empresa). Isto justifica a definição do IBGC "As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade."

Em 2001 houve um fato que acelerou a adoção de práticas de Governança Corporativa no mundo, que foram os escândalos financeiros de grandes empresas americanas como a Enron, que fraudava suas demonstrações financeiras para encobrir os prejuízos que ela vinha tendo, fazendo com que quando descoberto as fraudes, muitos acionistas perdessem o investimento de uma vida inteira. A Governança é baseada nos princípios da transparência, independência e prestação de contas (accountability) como meio para atrair investimentos para a organização.

E qual o papel da TI nessa Governança?

Pelo fato das informações financeiras das empresas estarem salvos em sistemas de informação, os gestores de negócio precisam ter garantias que as informações nestes sistemas são confiáveis. Para se ter uma ideia, após os escândalos de 2001, o congresso americano aprovou uma lei chamado *Sarbanes-Oxley*, mais conhecida como SOX, onde os executivos de empresas com ações na bolsa de Nova York são responsabilizados criminalmente por desvios nas demonstrações financeiras, podendo além de levar multa ser preso também. Mesmo que os executivos não tenham participação em fraudes das demonstrações financeiras, caso for detectado alguma fraude, eles são penalizados.

E como garantir que os dados nos sistemas são fidedignos (corretos)?

A Governança de TI tem o papel de criar estes controles de forma que a TI trabalhe de uma maneira o mais transparente possível perante os stakeholders (executivos, conselho de administração, acionistas). O framework, ou guia de melhores práticas mais utilizado no mundo em se falando de Governança de TI é o COBIT, mantido pela ISACA, que está na sua versão 4.1. O COBIT sugere uma série de processos a serem seguidos, chamados de objetivos de controle como: gerenciamento de incidentes, problemas, segurança da informação, indicadores, auditoria externa entre outros objetivos para que se possa garantir o controle das informações que se encontram em sistemas de informação.

A Diferença entre Gerenciamento de Serviços de TI e Governança de TI

"O **gerenciamento de serviços de TI** tem por objetivo prover um serviço de TI com qualidade e alinhado às necessidades do negócio, buscando sempre uma redução de custos a longo prazo". O Gerenciamento de Serviços de TI tem por objetivo **prover** ou **entregar serviços** através da implementação de processos na TI que suportem os processos do negócio. O framework mais utilizado e conhecido hoje é o ITIL. O Gerenciamento de Serviços de TI tem maior foco em responder a pergunta "como fazer?", ou seja, como implementar do que "o que fazer?", ou seja, o que implementar e como controlar. As suas métricas estão mais interessadas em medir o resultado dos processos em relação aos controles internos da TI do que aos processos do negócio.

Governança corporativa ou **governo das sociedades ou das empresas é o conjunto de processos**, costumes, **políticas, leis, regulamentos** e instituições **que regulam a maneira como uma empresa é dirigida**, administrada ou **controlada.**

A Governança de TI tem por objetivo dirigir e controlar as ações da TI, além disso, fazer com que os executivos do negócio sejam responsáveis pelo planejamento e resultados da TI, vendo a TI mais do seu lado estratégico. A Governança de TI faz com que os processos e metas de TI estejam alinhados com os processos de metas do negócio, pois as ações da TI estarão focadas nos principais processos do negócio. A Governança de TI está mais interessada em responder a pergunta "o que fazer?" do que em "como fazer?". O Framework mais utilizado hoje é o COBIT que está na sua versão 4.1. Uma empresa que adota a Governança de TI, irá utilizar os frameworks ITIL, PMBOK, CMMI, ISO27000 em conjunto com o COBIT para implementar os processos.

Resumindo tudo isso: o Planejamento, a direção e os controles que Governança de TI garante, juntamente com as boas práticas de implementação de processos de TI (ITIL, CMMI, PMBOK) o alinhamento entre TI e o negócio.

COBIT – Visão Geral

É o framework de Governança de TI mais utilizado no mundo. Ele está atualmente na sua versão 4.1, e com a versão 5.0 prevista para sair em 2012. A versão em português já está disponível no site da ISACA.

A ISACA segue a estratégia de outros frameworks que é disponibilizar uma parte do framework gratuitamente para os profissionais de TI, para que todos conheçam e tenham a necessidade/vontade de utilizá-lo, para depois "ganhar dinheiro" com material, treinamento, consultoria e etc. O material do COBIT utilizado para efetivamente implementar os processos, chamado "Control Practices" ou "Práticas de Controle" é somente para os membros que fazem sua contribuição anual.

Do que está disponível gratuitamente e que é também material de estudo para a certificação, este é dividido em 4 "partes". A primeira que é o sumário executivo é o introdutório da publicação, as 3 últimas existem para cada processo.

1) Framework ou Sumário Executivo

Esta parte do COBIT fala da importância de se gerenciar as informações das organizações devido o valor que elas têm hoje (que é maior que os ativos físicos muitas vezes). As organizações precisam também além de lidar com as informações geradas internamente, lidar com fatores externos como leis, regulamentos além de gerar informações confiáveis para os stakeholders em geral. O COBIT auxilia as organizações a suprir suas necessidades:

• Fazendo um link entre a TI e o negócio
• Organizando os processos e atividades de TI em um modelo mundialmente aceito.
• Identificando os maiores recursos de TI a serem gerenciados
• Definindo os objetivos de controle (ou processos) a serem considerados (implementados)

Em resumo, segundo esta publicação do COBIT prega que "para prover as informações que a organização precisa para atingir seus objetivos, recursos de TI precisam ser gerenciados por um conjunto de processos naturalmente (corretamente) agrupados".

2) Objetivos de Controle (Processos)

Os objetivos de Controle nada mais são que os processos a serem implementados. Na versão 4.1 do COBIT são sugeridos 34 processos, que estão divididos em fases, que são: "Planejar e organizar", "Adquirir e Implementar", "Entregar e dar suporte", e "Monitorar e avaliar o

desempenho da TI". Alguns processos sugeridos são bem conhecidos como: Gerenciamento de Incidentes, Problemas, Segurança, Backups, Gerenciar projetos, Mudança, Configuração entre outros.

A seguir a figura clássica do "guarda-chuva" abaixo:

O COBIT irá auxiliar na identificação de quais processos serão necessários implementar para o bom gerenciamento da TI, de modo que os executivos do negócio tenham o controle sobre a TI (sentido de transparência da Governança), e qual impacto da não implementação dos processos.

O COBIT não se preocupa em como irá ser implementado, e sim em o que será implementado. Na parte do "como serão implementados" é que entram os outros frameworks como ITIL, PMI, ISO27001 entre outros. O COBIT na verdade é um apanhado de processos dos mais variados frameworks. É um integrador de todos estes processos.

3) Orientação de Gerenciamento ou Management Guidelines

Nesta parte que o COBIT define as entradas, atividades dos processos e saídas que cada processo irá gerar. Além disso, se preocupa em definir as responsabilidades de cada atividade do processo através da matriz RACI (Responsible, Accountable, Consulted e Informed). O COBIT é uma biblioteca voltada a indicadores, e as orientações de gerenciamento sugerem para cada processo indicadores de desempenho de TI e de negócio. O COBIT sugere indicadores de negócio, pois cada processo de TI existe para suportar um ou mais processos de negócio.

4) Modelos de Maturidade

E no final da descrição de cada processo há um modelo de avaliação de maturidade do processo, que é dividido em "inexistente", "inicial", "Repetitivo mas intuitivo(não escrito) ,

“Definido”(escrito e comunicado), “Gerenciado e Medido”, e “otimizado”. Os modelos de maturidade são muito importantes para saber qual grau de maturidade de um dado processo na organização, além de se poder estabelecer através dele onde se quer chegar.

O COBIT tem mais algumas publicações complementares: guias de bolso, documentação sobre segurança, trilhas de auditoria entre outros, além de publicações como o framework VAL IT.

Este interessante framework vem sendo cada vez mais utilizado no mundo, pelos bancos e outras organizações que precisam cumprir leis e regulamentos como a SOX.

Os 5 focos da Governança de TI – Segundo o COBIT 4.1

As 5 áreas de foco da TI que o COBIT procuram atender uma eficaz e eficiente Governança de TI.

O COBIT é baseado na premissa de que a TI precisa entregar informação que a empresa necessita para atingir seus objetivos.

Segundo a publicação do COBIT 4.1 *"Essas áreas de foco em governança de TI descrevem os tópicos que os executivos precisam atentar para direcionar a área de TI dentro de suas organizações."*

E como o COBIT atende estas 5 áreas de foco?

Atende através dos 34 processos que ele traz. Cada processo atende de forma primária ou secundária uma ou mais áreas de foco. Por exemplo, o processo "PO7 – Gerenciar os Recursos Humanos de TI" atende de forma primária os focos "alinhamento estratégico" e "gestão de recursos". O alinhamento estratégico é obtido através de boa comunicação e transparência da organização para com as pessoas e também das ações de TI estarem alinhadas com as ações do negócio. A gestão de recursos neste contexto, é uma gestão ótima das pessoas no que tange questões como recrutamento, competências necessárias, treinamento, avaliação de desempenho até o desligamento. De forma secundária, o PO7 atende as áreas de foco "Gestão de Risco" e "Mensuração de Desempenho". As pessoas por serem recursos importantes nas organização são fontes de risco, e o risco precisa ser gerenciado. Um risco, por exemplo, é a execução de uma atividade importante na organização depender do conhecimento de uma pessoa, não ter o "backup". Em mensuração e desempenho, as pessoas precisam ser medidas sobre o resultado esperado. Todos os processos que geralmente tem interação humana também precisam ser medidos.

Um outro exemplo é o processo "AI6 – Gerenciar Mudanças" que tem como foco principal "Entrega de valor". A entrega de valor neste caso é obtida através da implementação de mudanças com o mínimo impacto na operação da organização. As mudanças são constantes para implementação de melhorias em sistemas para atendimento a novas leis e regulamentos por exemplo.

Para finalizar, vamos resumir o objetivo de cada uma das áreas de foco.

Áreas de Foco

Alinhamento estratégico

Segundo o COBIT *"foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização."* Os processos do estágio "Planejar e Organizar" tem grande foco no alinhamento estratégico. Isto não é por acaso, visto que o alinhamento só irá ocorrer com um bom planejamento das ações de TI, tendo como base o planejamento estratégico da organização.

Entrega de Valor

Segundo o COBIT *"é a execução da proposta de valor de TI através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, se concentrado em otimizar custos e provendo o valor intrínseco de TI."* Os estágios "Adquirir e Implementar" e "Entregar e Suportar" tem foco maior na entrega de valor. Os usuários/clientes percebem valor da TI através dos processos que tem contato direto com eles, como "Gerenciar Incidentes" e "Gerenciar Mudanças".

Gestão de Risco

Segundo o COBIT *"requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia."* Os estágios "Adquirir e Implementar" e "Entregar e Suportar" tem foco também na gestão de riscos, principalmente processos como Gestão de continuidade de serviços de TI, segurança de sistemas e gestão de serviços terceirizados. É importante o mapeamento dos riscos e ter planos para a mitigação destes riscos. Os processos do estágio "Planejar e Organizar" também representam um risco, visto que a falta de alinhamento das ações de TI com o negócio pode gerar por exemplo ações que não agreguem valor a organização.

Gestão de Recursos

Segundo o COBIT *"refere-se à melhor utilização possível dos investimentos e o apropriado*

gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas." Processos como Gestão de Capacidade, Gestão de pessoas e fornecedores procuram atender esta área de foco.

Mensuração de Desempenho

Segundo o COBIT esta área de foco *"acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de performance e entrega dos serviços, usando, por exemplo, "balanced scorecards" que traduzem as estratégia em ações para atingir os objetivos, medidos através de processos contábeis convencionais."* O COBIT traz junto com a descrição dos processos sugestões de indicadores baseados nas perspectivas do balanced scorecard nos níveis operacionais, táticos e estratégicos. Como diz Peter Druker, "o que não é medido não pode ser gerenciado." A implementação da governança de TI tem o objetivo de dar direcionamento nas ações de TI buscando alinhamento e exercer controle sobre elas. Este controle é conseguido através de indicadores. Importante que hajam indicadores não só operacionais, mas que tenham significado para quem toma decisão dentro da organização.

Certificação COBIT 4.1

A certificação Cobit é como a ITIL (sem prazo de validade)? Ou o profissional tem que atualizá-la de tempos em tempos?

A pessoa com certificado Cobit 4.1(a versão mais atual até o momento), será para sempre certificado nesta versão do Cobit. Para ser certificado nas outras versões, na 5 por exemplo que está para sair, a pessoa terá que estudar tudo novamente e fazer a prova.

Como fazer para se certificar? É necessário treinamento ou, assim como na ITIL, basta estudar e prestar o exame para conseguir o nível foundation?

O Cobit só tem o nível Foundation. Você não precisa fazer cursos oficiais para prestar o exame. Basta apenas fazer o download do material no site da ISACA, estudar e fazer a prova. Há bons cursos on-line também que podem ajudar neste processo.

Quanto custa ($) a certificação mínima?

O preço do exame é U$ 150,00 dólares. Mais "barata" que a do ITIL que é U$ 174,00 dólares.

Onde eu posso realizar as provas?

É uma das diferenças entre a prova do COBIT e da ITIL. A prova do Cobit você faz on-line. Você marca sua prova no site Cobit Campus. Você precisará preencher 3 documentos. Dois documentos antes da prova e um depois. Antes da prova, você irá preencher um cadastro com suas informações, e outro cadastro com informações do seu proctor. O proctor é a pessoa que irá "supervisionar" sua prova. Verificar se a pessoa que está fazendo a prova não está "colando" ou coisas do tipo. O proctor pode ser alguém do seu trabalho ou do seu curso. A prova tem que ser marcado com 10 dias de antecedência, com horário certo e no horário comercial (do Brasil). Depois da prova, você precisa enviar um documento em nome do proctor, atestando que você fez a prova dentro das regras (não ter colado). Toda esta tratativa pode ser feito via e-mail. Para marcar a prova é necessário ter cartão de crédito internacional.

Quais os detalhes da prova? (múltipla escolha?, número de questões, porcentagem para aprovação)

Você tem 60 minutos para responder 40 questões. Todas são de múltipla escolha. Até então as provas são somente em inglês, espanhol e japonês ou chinês. Em português não há ainda, apesar de já termos material em português. Para passar no exame, você precisa acertar 28 questões de 40, ou 70%. É preciso estudar a introdução e o sumário executivo para pegar bem os conceitos. Os processos principais a serem estudados são o PO10 e DS02. O restante dos processos, é necessário saber para que servem e os objetivos.

Lei Sarbanes-Oxley e a TI

A lei Sarbanes-Oxley foi criada nos EUA em 30 de Julho de 2002 pelos senadores Sarbanes e Oxley, sendo a lei batizada com a junção de seus nomes. O gatilho para a criação desta lei foram os escândalos financeiros ocorridos nos EUA. Algumas empresas, sendo o caso mais famoso da Enron, uma das líderes mundiais em distribuição de energia e comunicações da época e de faturamento de cerca de 100 bilhões de dólares no ano 2000, fraudou diversos demonstrativos fiscais e contábeis com auxílio de empresas e bancos, omitindo do seu balanço anual dívidas de cerca de 25 bilhões de dólares. Esta omissão fez com que investidores comprassem ações de uma empresa aparentemente rentável e sadia, sendo que a mesma estava á beira da falência, onde muitos perderam investimentos de uma vida (Nos EUA muitas pessoas investem em ações assim como no Brasil colocamos dinheiro na poupança). Para fazer com que a credibilidade nas aplicações na bolsa fossem melhoradas, a SOX surgiu.

Antes da SOX, somente as empresas eram punidas devido fraudes financeiras. Portanto, se o executivo cometia alguma fraude, passava ileso, sendo a empresa responsabilizada. A SOX responsabiliza civil e criminalmente os executivos do negócio em caso de fraudes, mesmo que eles não tenham participação direta. A ideia da SOX é que as empresas demonstrem eficiência na Governança Corporativa. A SOX define uma série de controles que são necessários para garantir a segurança, veracidade, integridade entre outros aspectos da informação.

A SOX afeta empresas que tem suas ações negociadas na Bolsa de Nova York. Algumas empresas brasileiras que tem as ações na bolsa de NY são: Petrobras, GOL, TAM entre outras.

E como esta lei afeta a TI?

Esta lei afeta diretamente a TI pelo fato de todas as informações financeiras serem guardadas em sistemas de informação. A SOX exige entre outras coisas que:

• *Estabelece regras de elaboração e publicações de resultados financeiros. Portanto os sistemas de informação precisam estar adequados para isso.*

• *O CEO e CFO precisam atestar e assinar que os relatórios financeiros estão corretos. Imaginem a pressão deles por controles adequados dos sistemas por parte da TI. Eles são responsabilizados em casos de erros, fraudes e etc.*

• *O conteúdo da informação precisa ser correto.*

• *A informação precisa estar disponível no momento correto (questões de disponibilidade).*

• *Acessível somente por pessoas autorizadas (segurança).*

• *Informação precisa estar atualizada.*

• *Os sistemas internos precisam ter controles relativos às informações, novas funcionalidades e permitir o rastreio (logs) no caso de erros em relatórios, alterações indevidas.*
• *Novos processos de TI precisam ser implementados para mitigar os riscos.*
• *Indicadores de desempenho precisarão ser criados.*
• *Entre outros aspectos.*

No pouco que listamos acima, podemos notar que processos maduros de desenvolvimento de software, gestão de serviços de TI, segurança da informação serão de fundamental importância para que a SOX seja cumprida. O COBIT, framework de governança de TI, será utilizado para "governar" e controlar todos estes processos, dando a visão gerencial á respeito da TI para os executivos, e fazer com que a TI esteja alinhada com o negócio de forma a cumprir a lei.

Ferramentas da Governança de TI: Gestão Portfólio de Projetos

Busca-se constantemente nos dias atuais o alinhamento entre TI e negócio. Como é possível alcançar isto? A Gestão de Portfólio de Projetos tem um papel muito importante para chegarmos neste alinhamento, ou integração como já se fala hoje. O objetivo principal desta disciplina é selecionar, controlar e validar os projetos, de modo que seja feito o alinhamento entre os objetivos do negócio (missão, visão, planejamento estratégico) e da TI.

São quatro os processos de Gestão de Portfólio de projetos. Estes processos de gestão têm o objetivo de evitar projetos que não estão alinhados as metas da organização, que não trazem os benefícios esperados, projetos que sejam aprovados pela simples briga de poder entre outras questões.

O contexto de análise de um portfólio de projetos atualmente é bastante conturbado, o que dificulta a análise baseado nas experiências passadas. A gestão de portfólio apresenta atualmente as seguintes características:

• Lida com incertezas;

• Mudanças constantes;

• Difícil comparação, pois tudo muda muito rapidamente. O que antes era inviável hoje é necessário;

• Recursos limitados;

Para que os projetos certos sejam selecionados e priorizados, bem como os recursos para execução, são necessários processos para este gerenciamento. Cada processo utiliza-se de ferramentas que irão auxiliar na realização das atividades.

Alinhamento

O alinhamento garante que os projetos reflitam os objetivos que a organização deseja alcançar, sejam eles financeiros ou não financeiros. Uma ferramenta utilizada para geração do alinhamento é o Balanced Scorecard. O BSC como é conhecido, garante que as metas do negócio estejam relacionadas através dos aspectos “Aprendizagem e crescimento”, “Processos Internos”, “Visão do cliente” e “Financeiro”. Estas metas poderão ser utilizadas para análise de seleção e priorização dos projetos.

Seleção

A seleção irá buscar dentro dos objetivos da organização, sua cultura e visão, quais oportunidades/projetos deverão ser priorizados. As ferramentas utilizadas para selecionar os projetos que irão compor o Portfólio são:

• Aderência e Contribuição às estratégias.

• Avaliação Financeira

- Pay back
- Valor Presente
- ROI
- Avaliação de Benefícios não quantificáveis
- Avaliação de restrições.

Na seleção, além das técnicas de seleção e priorização de projetos, pode-se utilizar a intuição para a tomada de decisão. Utilizando a intuição iremos geralmente nos basear em experiências passadas, ou troca de informações. Isto pode se tornar muito perigoso visto que é sabido o benefício de um dado projeto pode mudar de acordo com o tempo, mercado, ameaças, oportunidades e etc.

Controle

O que não se mede não se gerencia, resumindo, o que não se mede não se controla. Este processo tem por objetivo acompanhar a execução dos projetos em questões como: custos, prazos, tempo, escopo, qualidade, recursos humanos entre outros. Como ferramenta, pode ser utilizada melhores práticas de Gestão de Projetos - PMI ou metodologias como PRINCE2. Para cada atividade realizada dentro do processo se definem indicadores, onde os indicadores garantirão o controle e darão informações para tomada de decisão.

Validação

A validação irá identificar se os projetos realizados atingiram seus objetivos definidos no alinhamento estratégico através do BSC, se alcançaram os objetivos do negócio. A validação estende a verificação do cumprimento do projeto (custos, prazo, qualidade) para validar se os mesmos estavam alinhados realmente com os objetivos do negócio propostos, se tiveram o retorno de valor esperado, seja ele financeiro ou não-financeiro.

Devido os altos investimentos em TI atualmente, é muito importante que tenhamos processos eficazes para que tempo e dinheiro não sejam “jogados fora”. Como sabemos, verificar erros no planejamento é muito mais barato do que identificar durante a execução ou ao final dela. Por isso a Gestão de Portfólio de projetos se torna uma ferramenta tão interessante para execução da Governança.

ITIL: Gerenciamento de Incidentes X Gerenciamento de Problemas

Esse assunto está presente na vida de muitos profissionais de TI, que apesar de serem parecidos tem focos diferentes, e saber quanto investir de tempo em cada processo pode ser a receita do sucesso na sua empresa: Gerenciamento de Incidentes e Gerenciamento de Problemas. O processo de gerenciamento de incidentes tem o objetivo de restaurar a operação normal de um serviço o mais rápido possível. Este processo tem grande importância para que os Acordos de Nível de Serviço sejam cumpridos. O Gerenciamento de Problemas tem por objetivo encontrar a causa de um ou mais incidentes de forma a erradicá-los da infraestrutura, evitando a recorrência dos incidentes e melhorando o atendimento aos Níveis de Serviço. Menos incidente maior disponibilidade.

O assunto Gerenciamento de Incidentes é padrão nos Service Desk Brasil afora, o que não vejo a respeito do Gerenciamento de Problemas. A questão custo e ter equipes geralmente enxutas contribuem para isso. Apesar de não se falar muito em gestão de problemas, esta é uma atividade que sempre fizemos. O que há hoje é que tratamos problemas dentro dos incidentes. Ficou confuso? Vou explicar melhor. Tratar problema dentro de incidente é após você restaurar a operação do serviço, deixar o "chamado", "ticket" ou "incidente" aberto para encontrar a causa do incidente e através deste "chamado" resolver o problema de forma a evitar novos incidentes. O que a ITIL prega é que restaurado o serviço o "Incidente" seja encerrado, e um problema seja aberto, relacionando o ID do "Incidente" com o ID do "Problema" para que seja analisada a causa. Então nós sempre tratamos problemas, apesar de não ter um processo definido certo? Sim. Mas por não existir geralmente um processo de Gestão de Problemas definido e separado de Incidentes, deixamos de colher informações importantes e melhorar nossa tomada de decisão. Tratar incidentes e problemas no mesmo "chamado" faz com que saber o tamanho da fila de incidentes e problemas fique "impossível". Saber quantos incidentes e quantos incidentes que "viraram" problemas os atendentes tem na fila também. Tirar um relatório de tempo médio de resolução dos incidentes então? Fica totalmente distorcido.

Qual a solução?

A solução é separar de fato os processos de gestão de incidentes e gestão de problemas. A equipe a ser utilizada pode ser a mesma, mesmo que isto não seja o recomendado pela ITIL. A solução é que sua ferramenta de Service Desk permita que Incidentes e Problemas sejam tratados separadamente, relacionando somente os IDs e Itens de Configuração dos Incidentes aos dos Problemas de maneira simples, para poder saber quantos incidentes estão relacionados ao problema, auxiliando assim na definição de prioridade para resolução dos problemas. Se temos os processos

de G. Incidente e G. Problema definidos e os resolvedores são os mesmos, quanto tempo devo dedicar para cada processo ? Segundo a ITIL: “O seu negócio deve definir”. Alguns dizem que a ITIL sugere que 80% do tempo se resolvam incidentes e 20% problemas, mas não está na documentação. Com processos separados e com o correr do tempo, você irá conseguir extrair informações importantes e poder analisar quanto tempo dedicar para cada processo.

Implementar o processo de Gerenciamento de Problemas é mais uma questão de organização do que “fazer mais coisas com o mesmo número de atendentes”, isso claro se sua ferramenta de Service Desk permitir de uma maneira simples, senão concordo que isto vira um pesadelo! Os benefícios desta separação para a equipe e para os tomadores de decisão são muitos, desde melhora no moral da equipe, passando aumento da maturidade do Service Desk e informações mais precisas para os tomadores de decisão.

Na sua empresa, quais processos existem no Service Desk? Incidentes? Problemas?

ITIL: O que muda entre a versão 2 e 3 ?

A versão 3 da ITIL foi lançada em 2007, apesar disso, a maioria das implementações nas organizações são baseadas na versão 2. Isso porque os conceitos e processos são mais fáceis de serem entendidos e implementados, e todo o investimento feito até então não pode simplesmente ser deixado de lado.

A OGC, foi muito feliz no lançamento desta nova versão. A ITIL V3 é uma grande evolução da versão anterior. O núcleo da ITILV2 eram os livros de "Entrega de Serviços" e "Suporte a Serviços". Nesta abordagem, não havia uma sequência clara de implementação dos processos, e nem um foco muito grande em estratégia e melhoria dos processos.

A versão 3 pega todos os 10 processos e uma função da ITIL v2 e os distribui em 5 estágios/livros:

- Estratégia de Serviço
- Desenho de Serviço
- Transição de Serviço
- Operação de Serviço
- Melhoria Continuada

Os processos da ITILV2 foram distribuídos dentro destes estágios, novos processos foram criados, e outros foram "desmembrados". Por exemplo, na versão 2, o processo Gerenciamento de Capacidade tinha uma atividade que era o Gerenciamento da Demanda. O Gerenciamento de Capacidade na versão 2 misturava a gestão da Capacidade dos itens de configuração(técnico) com o monitoramento do negócio por serviços de TI(gestão). Na versão 3, o Gerenciamento de Demanda virou um processo a parte e foi colocado no estágio estratégia de serviço. A ideia é pensar na demanda que certo serviço terá, antes mesmo do desenho e configuração do mesmo.

A ITIL V3 pensa no ciclo de vida do serviço, já que todo serviço nasce a partir de uma necessidade do negócio (novos produtos, novas tecnologias que aumentam produtividade, reduzem custos e etc), é desenhado, utilizado e descartado quando não tiver mais utilidade, ou quando outra tecnologia assumir seu lugar.

Falando resumidamente sobre os estágios, a estratégia tem o foco em verificar o valor (benefício/retorno) de um novo serviço para o negócio, bem como os custos envolvidos e sua demanda. O desenho irá fazer a configuração dos itens de configuração que juntos irão formar um serviço, levando em conta requisitos de disponibilidade, continuidade dos serviços entre outros pontos, identificados na estratégia. O estágio de transição terá a responsabilidade de construir os serviços e disponibilizá-los no ambiente de produção de forma segura. A operação de serviço terá

foco em manter os serviços funcionando. A melhoria contínua tem o foco ajustar os serviços de acordo com as mudanças do negócio, além de atuar na melhoria contínua de todos os processos em todos os estágios.

A figura que representa todo este ciclo de vida é a abaixo:

ITIL e o ciclo de vida: Estratégia do Serviço

Estamos iniciando uma série que irá detalhar cada estágio do ciclo de vida do serviço proposto pelo ITIL. No dia de hoje vamos falar sobre a Estratégia do Serviço.

O principal objetivo da estratégia do serviço é fornecer as diretrizes para os outros estágios do ciclo de vida do serviço, e transformar o Gerenciamento de Serviços em um ativo estratégico, de grande importância para a organização. É pensar em todas as demandas e necessidades por serviços antes de colocar a mão na massa efetivamente. Nós de TI estamos acostumados em primeiro fazer e depois pensar em quem irá utilizar, quando, de onde e etc, desperdiçando muito tempo e recursos sem o devido retorno. A estratégia irá definir onde o provedor de serviços está, aonde quer chegar e o que fazer para chegar ao objetivo. O livro estratégia de serviço foca bastante em uma série de conceitos no que tangem os serviços de TI:

Valor do Serviço = Utilidade + Garantia

Para que um cliente perceba um benefício em um serviço, e perceba o valor dele é necessário que este serviço seja útil, ou seja, que traga uma facilidade ou que elimine uma restrição e também necessita da garantia de que este serviço esteja disponível quando necessário. Para ilustrar este cenário, pense na telefonia móvel. A utilidade do serviço é toda mobilidade que ela dá, permite fazer ligações, receber mensagens, e-mails de onde a pessoa estiver. A garantia é o serviço de e-mail e a qualidade do sinal estarem disponíveis quando necessário e na qualidade esperada.

Ativos de Serviço

Os ativos de serviço estão divididos em dois grupos:

1) Recursos: Financeiro, Infraestrutura, Aplicativos, Informação e Pessoas

2) Habilidades: Gerenciamento, Organização, Processos, Conhecimento e Pessoas.

Um ativo de serviço se torna um ativo estratégico quando as habilidades necessárias são utilizadas para gerenciar os recursos disponíveis. Pessoas são os ativos mais importantes.

Risco

Risco é uma incerteza, e por isso precisa ser bem gerenciado. Risco pode ser uma ameaça ou uma oportunidade. Um novo serviço pode ser uma ameaça, pois pode não vingar no mercado, mas pode ser uma oportunidade de sair na frente dos concorrentes em um dado mercado.

Os 4 Ps da estratégia

Perspectiva: É a visão da organização. Na perspectiva se define qual a missão, a visão e os valores.

Posição: Como o provedor de serviços quer ser reconhecido pelo mercado. Alguns exemplos seriam por causa de um serviço em específico, pelo custo baixo, pela qualidade do serviço.

Plano: É a execução da estratégia para alcançar a visão desejada.

Padrão: São os processos e a organização para que a perspectiva, posição e planos sejam cumpridos.

A estratégia do serviço traz 3 processos:

Gerenciamento de Portfólio de Serviços

O Portfólio de serviços irá fazer o controle de todos novos serviços solicitados, em desenvolvimento, em produção e aposentados. O portfólio de serviços irá utilizar de algumas ferramentas para analisar a viabilidade de um serviço como ROI, Caso de Negócio, análise SWOT e entre outros. O Portfólio de serviços se preocupa em responder algumas perguntas como: Porque um cliente compraria de nós um serviço? Porque compraria de nós? Qual preço estaria disposto a pagar?

Gerenciamento da Demanda

O Gerenciamento da demanda tem o objetivo de "prever" a demanda atual e futura dos serviços. Devido à natureza não estocável dos serviços, ou seja, o serviço ser consumido no mesmo tempo que é gerado, é importante que seja sabida a demanda do serviço ao longo do tempo para que a quantidade de recursos adequados seja alocada. Como exemplo, pense num site de e-commerce como a **americanas.com** durante dia das mães, das crianças e natal. Com certeza o volume de compras é bem maior do que nas datas "normais".

Sabendo da demanda do serviço, é possível influenciar a utilização dos mesmos através da cobrança, por exemplo, otimizando a utilização dos recursos

Gerenciamento Financeiro

O Gerenciamento Financeiro tem o objetivo de assegurar os recursos necessários para entrega dos serviços de TI, e fornecer as informações de custo da provisão dos serviços e o preço a ser pago pela utilização. O Gerenciamento Financeiro é estratégico para tomada de decisão sobre os investimentos em TI.

O Livro estratégia de Serviço sugere algumas fórmulas para calcular o ROI esperado de cada serviço na linha do tempo. É importante ter em mente que um acionista que coloca dinheiro em uma empresa, espera que o seu dinheiro investido tenha um retorno com "juros" e "correção monetária". Vale lembrar que o dinheiro investido em TI poderia ser utilizado na compra de um carro, imóvel ou investimento na bolsa de valores por exemplo. Analisando por este prisma, vemos a importância do Gerenciamento Financeiro para a estratégia do serviço e o Gerenciamento de Serviços como um todo.

A estratégia do serviço irá fazer o alinhamento entre TI e o Negócio, direcionando todas as ações e recursos para o desenho, transição, operação e melhoria dos serviços.

ITIL e o ciclo de vida: Desenho do Serviço

O segundo estágios do ciclo de vida do serviço: O Desenho do Serviço.

A publicação "Desenho do Serviço" tem como foco o desenho e o desenvolvimento de serviços e os processos de gestão de serviços de TI. Sim! É no desenho que iremos desenhar de fato os processos de Gestão em TI: Gerenciamento de Incidentes, Problemas, Gerenciamento de Portfólio e Catálogo de Serviços entre outros, com grande ênfase nestes dois últimos. Este estágio cobre princípios de desenho e métodos para converter objetivos estratégicos em serviços no portfólio e utilizáveis pelos clientes dentro dos SLAs acordados. O escopo deste estágio não está limitado a novos serviços. Inclui também mudanças e melhorias necessárias para aumentar ou manter o valor que os clientes obtêm dos serviços ao longo do ciclo de vida.

O gatilho deste estágio serão mudanças no negócio. Mas como? A necessidade de novos serviços para suportarem novos processos de negócio, novos produtos ou a necessidade de que os serviços atuais sejam remodelados para atender novas demandas que irão gerar a necessidade de novos desenhos ou a revisão deles.

Após aprovação do novo serviço no estágio da Estratégia é necessário além de incluí-lo no Catálogo de Serviços, arregaçar as mangas e desenhar como este novo serviço(quais componentes utilizar? Em qual disposição?) irá suportar esta nova necessidade, levando em consideração os Níveis de Serviços necessários, disponibilidade, capacidade, continuidade, segurança entre outros.

Mas o desenho não irá se preocupar somente com a arquitetura do serviço. Irá se preocupar também em como mensurar este novo serviço, os processos necessários para suportá-lo na operação, o conhecimento necessário da equipe, critérios de aceite entre outros. Todas estas informações estarão contidas no "Pacote de Desenho de Serviço" que será o principal entregável deste estágio e utilizado durante o restante do ciclo de vida (Transição e Operação).

Alguns conceitos que esta publicação do ITIL nos traz:

4 Ps

No estágio desenho de serviço, temos os 4 Ps, que envolvem:

- Pessoas: Papéis a serem atribuídos a pessoas nos processos.
- Processos: Processos definidos e que sejam medidos.
- Parceiros: Fornecedores
- Produtos: Que englobam serviços, tecnologia e ferramentas.

5 Aspectos do desenho

- Serviços novos ou alterados.

- Sistemas de Gestão de Serviços e ferramentas, principalmente o portfólio de serviços, incluindo o Catálogo de Serviços
- Arquitetura do serviço. Qual a disposição dos componentes necessária.
- Os processos necessários para suportar o serviço.
- Métodos de medição e métricas, necessário para geração da melhoria continuada. Como dia Peter Drucker: "*O que não se pode medir*, *não pode se gerenciar"*.

Atividades deste estágio

1) Analisar requisitos, documentar e acordar (Recebidos da estratégia – Portfolio)
2) Desenhar a solução
3) Avaliar soluções alternativas
4) Adquirir a solução preferida
5) Desenvolver a solução (make or buy)

Processos:

Catálogo de Serviços:

No catálogo de serviços irão constar todos os serviços em produção e os serviços do portfólio já aprovados. Interessante que o catálogo de serviços tenha duas faces: a do cliente e a da equipe de TI. No catálogo devemos ter a descrição dos serviços, quais os SLAs relacionados, quais itens de configuração que suportam quais processos de negócio entre outras informações.

Gerenciamento de Nível de Serviço

Este processo irá fazer o alinhamento de expectativas entre o cliente e área de TI. O gerente de Nível de Serviço terá a incumbência de buscar do cliente quais suas necessidades em relação aos serviços e desenhar os acordos entre cliente e TI, TI e áreas internas e entre TI e fornecedores, de modo que os SLAs sejam atingidos. Estes acordos firmarão metas de disponibilidade, desempenho para os serviços, além de acordar sobre tempos de resolução dos incidentes por exemplo.

Gerenciamento de Disponibilidade

Este processo irá auxiliar no atendimento dos SLAs acordados entre TI e o cliente, monitorando a disponibilidade dos itens de configuração. Não devemos confundir gerenciamento de disponibilidade com Gestão de Continuidade no negócio. Este processo traz indicadores bem conhecidos como: disponibilidade do serviço, tempo média para reparo e tempo médio entre incidentes do serviço.

Gerenciamento de Capacidade

Este processo é dividido em 3 sub-processos:

- Capacidade do Negócio: Acompanha as necessidades atuais e futuras no negócio através do

planejamento estratégico da organização.

- Capacidade do Serviço: Monitora o serviço de ponta-a-ponta.
- Capacidade do Componente: Monitora a utilização de todos os componentes que formam o serviço.

O objetivo do Gerenciamento da Capacidade é acompanhar o desempenho atual e planejar capacidade futura. Quando o custo/benefício for justificável, aperfeiçoar a utilização dos recursos atuais.

Algumas atividades deste processo:

- Monitoramento e geração de relatórios sobre o desempenho atual dos serviços e componentes.
- Auxiliar outros processos como Gestão de Problemas, mudanças e incidentes em questões relacionadas à capacidade.
- Garantir que se tenha a capacidade adequada para suprir a demanda atual e futura do negócio por serviços de TI.
- Prever utilização futura de infraestrutura e aplicações através de técnicas de análise, sizing, modelagem entre outros.

Gerenciamento de Continuidade

Este processo é uma extensão do Gerenciamento de Continuidade do negócio, e tem como missão garantir a continuidade dos serviços essenciais em casos de sinistros e incidentes graves quando o custo/benefício justificar.

Gerenciamento da Segurança da Informação

Garantir no processo de desenho do serviço que se atente para aspectos de confidencialidade, integridade e disponibilidade (CID) dos serviços. O principal produto deste processo é a Política da Segurança da Informação, que tem como base a ISSO 27001.

Gerenciamento do Fornecedor

O Gerenciamento de Fornecedor auxilia no processo de prospecção de fornecedores, além de registrar todos os contratos e participar do processo de assinatura, revisão e cancelamento dos contratos de fornecedores de TI.

Para concluir, podemos afirmar que os reflexos de um serviço bem desenhado serão percebidos na operação de serviço e com certeza neste ponto se economiza muito dinheiro, e o contrário também é verdadeiro.

Sua empresa, desenha o serviço antes de colocar em produção? Ou os coloca em produção e depois sai apagando o incêndio?

Amadurecendo com o CMMI para desenvolvimento

O CMMI para desenvolvimento é um importante modelo de referência, importante ferramenta da Governança de TI. O CMMI-DEV, ainda pouco difundido no Brasil é um modelo integrado de referência que contém práticas genéricas e específicas para tudo que envolve o desenvolvimento de sistemas (seriam os como os processos no ITIL, COBIT), concebida pelo SEI (Software Engineering Institute). Seus principais utilizadores hoje são "software houses", ou empresas onde o desenvolvimento interno e aquisição tenham um grande impacto no negócio.

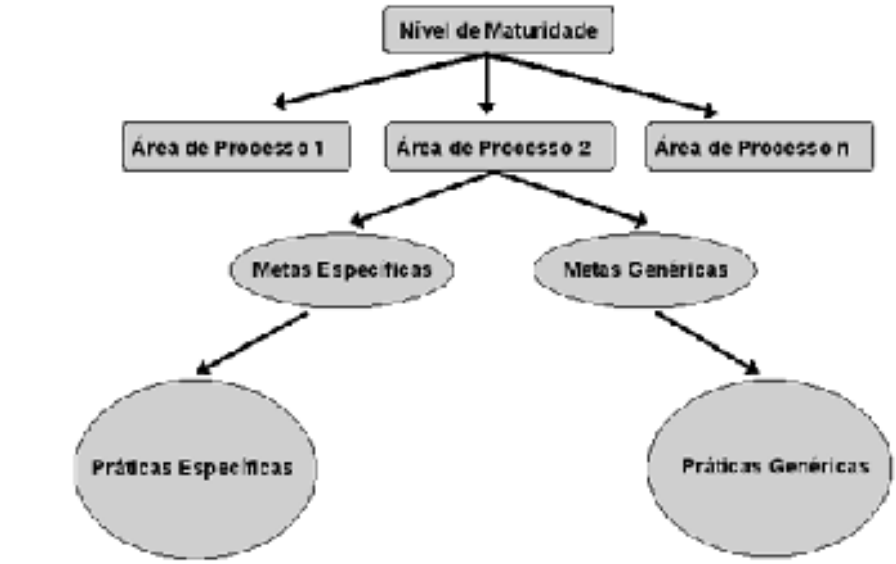
O CMMI tem como objetivo aumentar o nível de maturidade da organização através de metas e melhoria contínua dos processos, trazendo uma melhor coordenação do processo de desenvolvimento como um todo, desde o levantamento de requisitos, passando pela gestão de projetos até a manutenção do produto, e muito importante, disseminando a cultura do medir para melhorar. A aplicação de modelos de qualidade como o CMMI traz uma série de benefícios, conforme relatado pelo SEI:

- Redução de custos em 20%.
- Aumento de 37% no atendimento de prazos.
- Aumento de 62% na produtividade
- Aumento de 50% da qualidade
- Aumento de 14% na satisfação dos clientes
- Relação de 5:1 do ROI

A ideia do CMMI é integrar várias práticas utilizadas antes em separado para o desenvolvimento de sistemas. O CMMI não é um modelo de desenvolvimento de software, ele tem uma abrangência muito maior do que isso, tendo como foco 4 categorias, e cada categoria tem uma série de processos relacionados, os quais listo alguns aqui:

• **Gestão do Processo:** Foco no processo organizacional, Treinamento organizacional.
• **Gestão do Projeto**: Planejamento do Projeto, Gestão Integrada do Projeto, Gestão de Riscos.
• **Engenharia:** Desenvolvimento de requisitos, Gestão de requisitos.
• **Suporte:** Gestão da Configuração, medição e análise, análise de resolução as causas.

A estrutura do modelo segue conforme abaixo:



O CMMI tem duas abordagens para sua implementação:

Abordagem Por estágios

Nesta abordagem, cada Nível de maturidade tem uma série de áreas de processo que precisam ser atendidas, de cada uma das 4 categorias. O CMMI sugere que as empresas que estão iniciando no modelo e que tem pouca maturidade iniciem pelos processos de gerenciamento de projetos, pois para o SEI, para quem está iniciando o mais importante é ter controle de qualidade, prazo e custos dos projetos, para depois partir para os outros níveis de maturidade.

Os níveis de maturidade na abordagem por estágio são os abaixo:

1 – Inicial (Todas as organização)

2 – Gerenciado (foco em Praticas de gestão de projetos)

3 – Definido (engenharia de produtos)

4 – Gerenciado quantitativamente – métricas (medição e análise)

5 – Otimizado (inovação organizacional)

Abordagem Contínua

Na abordagem contínua, a implementação dos processos é executada um a um, geralmente utilizada por empresas de menor porte. Esta abordagem permite que o custo da implementação do modelo CMMI seja diluído no decorrer do tempo, e a certificação de maturidade é por processo.

Para implementação do modelo CMMI, pode-se utilizar também uma abordagem que une a abordagem contínua e por estágios, mais conhecida como “target staging”, implementando inicialmente alguns processos, tendo como objetivo atingir algum nível de maturidade da abordagem por estágios.

Governança de TI: É preciso “evangelizar”!

Segundo uma pesquisa realizada pelo MIT “só 38% das (grandes) empresas brasileiras têm governança de TI”, enquanto governança na área de finanças é de 95%. Isso me diz duas coisas:

1. O Brasil está atrasado nas práticas de governança corporativa de TI, o que revela em muitos casos pouca preocupação com as informações das empresas, gerando altos riscos de segurança.
2. Existe muito trabalho a ser feito, portanto, há muito para ser explorado! Ou seja, é uma oportunidade de negócio para profissionais dessa área.

A governança de TI, nada mais é do que a utilização de boas práticas de gerenciamento de TI, não apenas pelos gestores de TI, mas pelos gestores dos negócios.

Não é fácil para muitos gestores de negócio entender porque precisam investir na sua infraestrutura de TI. É comum ouvir coisas do tipo: “nunca gastei dinheiro com TI, porque agora irei fazê-lo?”, muitos só entendem que é necessário investimento quando incidentes ocorrem, causando a indisponibilidade de serviços essenciais para o negócio e a empresa perde muito dinheiro ou mesmo quando perdeu a base de dados de clientes, cobranças e outras informações estratégicas, perdendo mais do que dinheiro e sujando a imagem da empresa. A governança de TI tem o papel de mostrar os custos e benefícios envolvidos no gerenciamento de TI. Se dentro das grandes corporações somente 38% das empresas brasileiras tem efetivamente uma preocupação com este assunto, imaginem as pequenas e médias!!!

Existem muitas matérias dizendo que os CIOs, ou gerentes de TI, devem ser uma espécie de “evangelizadores” dentro das suas empresas, pois precisam mostrar para os gestores do negócio o valor que a TI pode ter e os riscos existentes de um falho gerenciamento dos recursos de TI: pessoas, aplicações, informações e infraestrutura. Traça-se um paralelo entre os CIOs e as empresas prestadoras de serviços em TI. É a nossa missão como prestadores de serviço abrir os olhos de nossos clientes para estas questões, que para nós são tão simples, porém, para os gestores de negócio é um assunto difícil de ser assimilado e entendido. Vejo que cada vez mais precisamos deixar a linguagem técnica um pouco de lado e falar mais com uma linguagem que os gestores de negócio entendam o custo/benefício de uma ótima governança de TI e com isso adquirir maior confiabilidade e fidelidade de nossos clientes, e claro, aumentarmos nossas receitas.

Governança e a Gestão de Riscos em TI

Um assunto que vem ganhando muita atenção nestes últimos tempos, isto em função das constantes transformações que as organizações estão inseridas (também em TI) e nesta economia globalizada e instável que estamos vivendo: a gestão de riscos de TI.

Para antes entrar efetivamente no assunto, vamos primeiramente entender o que é um risco.

> *"O termo Risco é utilizado para designar o resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento, aleatório, futuro e que independa da vontade humana, e o impacto resultante caso ele ocorra. É também uma a probabilidade de ocorrência de um determinado evento que gere prejuízo econômico."*

O termo "prejuízo econômico" já nos diz tudo. Podemos dizer que as empresas assumem riscos ao colocar produtos ou serviços novos no mercado. Um risco pode ser classificado como uma oportunidade e/ou uma ameaça. Uma empresa corre o risco de ganhar muito dinheiro com o novo produto/serviço (oportunidade) ou corre o risco de ter um grande prejuízo (ameaça). Grande parte dos riscos fogem do controle das empresas, portanto, a única opção é ter planos para caso os riscos se tornem verdade. A importância de se analisar os riscos cresce a cada dia. Um exemplo é o que acontece quando às bolsas brasileiras são afetadas pelas crises em outros lugares, como Grécia e Irlanda. O mundo globalizado é isto.

Os termos "risco", "análise de risco", "gestão de risco" vem ganhando espaço dentro das organizações. Podemos dizer que praticar Governança seja ela empresarial, seja de TI ou de outra área, também é através ferramentas, processos e estruturas organizacionais diminuir os riscos de algo inesperado e ruim acontecer.

Na área de TI, podemos encontrar referências sobre como mitigar/controlar riscos no PMBOK, ITIL, COBIT entre outros frameworks. Temos frameworks focados em gestão de riscos como o M_O_R da OGC que é a mesma mantenedora da ITIL e o Risk IT que foi concebida pela ISACA, mesma mantenedora do COBIT.

Um dos acontecimentos mais conhecidos relacionados à mitigação de riscos é o "Acordo de Basiléia I" de 1988 na cidade de Basiléia na Suíça. O acordo de Basiléia tem o objetivo de fixar índices, criando uma padronização financeira mundial, tendo como objetivo diminuir o risco operacional, e consequentemente o risco das instituições financeiras "quebrarem". Um exemplo do acordo é que os bancos só podem emprestar 12 vezes o valor de seu capital e reservas. Em 2004 o acordo ganhou sua segunda versão, o Basiléia II, trazendo melhorias nas regras estabelecidas. Existem uma série de outras regras, entre elas regras que impactam diretamente a área de TI.

Alguns pontos que o Acordo Basiléia II impacta em TI são: capacidade de armazenamento de dados, integridade das transações, segurança, contingência, planejamento da capacidade,

integridade na emissão de relatórios entre outros.

A Gestão de Riscos de TI precisa estar no dia-a-dia dos CIOs através de: processos que precisam ser implementados para mitigação de riscos, ajustes na estrutura organizacional para acomodar estes novos processos, definição de indicadores "de riscos", incluir a análise de riscos no Plano Diretor de TI ou Plano de Tecnologia da Informação, fazendo com que este assunto seja recorrente dentro da TI.

A primeira norma mundial (similar a ISO) referente Gestão de Riscos é a AS/NZS 34, elaborada em 1999. As etapas da gestão dos riscos são divididas em 2 fases: Identificação e avaliação.

Fase 1) Identificação

Estabelecimento do contexto: Relacionada ao escopo da avaliação que será realizada. Dentro de qual cenário o risco será analisado. Exemplo: E se uma enchente ocorrer em Blumenau?

Identificação de Riscos: É identificar o que pode dar errado dentro do escopo definido. O que uma enchendo afetaria na nossa organização para clientes e colaboradores?

Análise dos Riscos: Quais as consequências do risco caso ocorra. Dentro da análise dos riscos, temos 2 sub-atividades:

Análise qualitativa dos riscos: Identificar o impacto que certo risco poderá trazer para a organização e qual a probabilidade dela ocorrer.

Análise quantitativa: Estimar em valores $$ o quanto este risco poderá custar para a organização.

Fase 2) Avaliação

Plano de Resposta aos Riscos: Diante de um risco pode-se tomar 4 tipos de ação.

Evitar: Tomar uma ação para evitar totalmente um risco. Por exemplo, proibir o acesso a internet dentro da organização. Isto evita que vírus sejam copiados da internet.

Transferir: Pode-se transferir o risco para um terceiro. Exemplo: passar a administração de um servidor para um terceiro, e colocar em contrato penalidades caso o acordo estabelecido não seja cumprido.

Mitigar: Tomar ações para minimizar riscos. Exemplo: Limitar o uso da internet para alguns sites confiáveis somente.

Aceitar: Existem alguns riscos que são tão caros de serem "combatidos" que vale mais á pena aceitar o risco e ter um "plano B" para caso o mesmo ocorra. Exemplo: Guardar backup fora da empresa caso algum sinistro ocorra. Isso é geralmente utilizado pois o custo de se ter uma

estrutura de TI de continuidade a parte não justifica (que é a realidade da maioria das organizações).

Guarda-se somente um backup fora da empresa para restaurar o ambiente caso o sinistro ocorra.

Monitorar e controlar os Riscos: Acompanhar o dia-a-dia, fazendo o monitoramento dos riscos atuais e identificando novos riscos. Esta etapa também tem o objetivo de verificar se as políticas e procedimentos quanto a gestão dos riscos estão sendo seguidas. Também os indicadores referentes riscos são acompanhados nesta etapa.

Bem, a gestão de riscos é um processo importante e contínuo, e deve fazer parte da estratégia das organizações, já que como sabemos, os riscos de TI, não são de responsabilidade somente de TI, mas sim de toda a organização, principalmente dos tomadores de decisão.

Governança de TI: Segurança da Informação – normas ISO 27000

Segurança da Informação é assunto importante nas organizações hoje, e que precisa ter uma atenção especial do ponto de vista da Governança de TI: a segurança da informação. De acordo com uma pesquisa de 2006 com empresas norte americanas do Computer Security Institute – CSI em conjunto com o FBI as perdas relacionadas com segurança somaram um total de US$ 56 milhões.

No Brasil, a cert.br estimou que em 2005 há estimativa de perdas por fraudes chegou a R$ 300 milhões. A segurança da informação é padronizada através da norma ISO 27000, que tem por objetivo a proteção das informações organizacionais e ativos de TI. Para muitas empresas, as informações tem mais valor do que os ativos físicos.

Os mais variados frameworks como o ITIL no estágio Desenho de Serviço e o COBIT 4.1 no processo DS5 "Assegurar a segurança dos Sistemas" e DS12 "Gerenciando o ambiente físico" e a ISO 20000 entre outros também abordam o assunto, sempre com base nas normas ISO da família 27000.

Na família ISO 27000 temos duas normas que são as mais conhecidas:

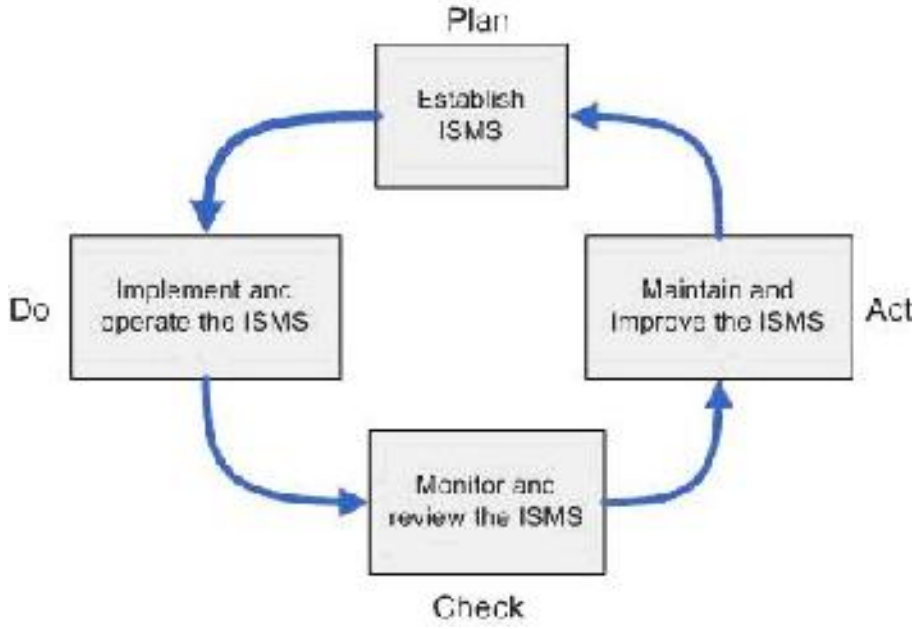
ISO 27001: É um modelo focado em estabelecer, implantar, operar, monitorar, rever, manter e melhorar um sistema de Gestão da Segurança da Informação. Irá implementar os controles da ISO 27002.

ISO 27002: Código de práticas para Segurança da Informação.

A ISO 27001 traz a abordagem da implementação segurança da Informação dentro de uma abordagem de processos que procura enfatizar aos usuários:

- O entendimento dos requisitos e a necessidade de se ter uma política da segurança da informação.
- Implementar e operar controles para gerenciamento dos riscos
- Monitorar o desempenho e a eficácia da política de segurança da informação.
- Promover a melhoria contínua.

Esta abordagem de processos é feita com base na tão conhecida estrutura PDCA, conforme temos na figura abaixo:



PDCA da Segurança

Planejar: Definição do escopo do sistema de gerenciamento de segurança da informação. Identificação de riscos, analisar e avaliar riscos, opções de tratamento de riscos entre outros.

Implementar e Operar: Plano para tratamento de riscos, implementação de controles, medição da eficácia dos controles.

Monitorar e revisar: Monitoramento e controle, revisões periódicas no sistema de segurança, conduzir auditorias internas, atualizar planos de segurança.

Manter e melhorar: Implementar melhorias identificadas, tomar ações corretivas e preventivas, aplicar lições aprendidas, comunicar as ações de melhoria aos interessados.

A ISO 27002 está estruturada em seções. Cada seção abaixo tem uma série de controles que podem ser implementados, que vai depender do tamanho e necessidade de cada empresa. No total, são cerca de 130 controles que podem ser implementados, divididos entre as seções abaixo.

- Política da segurança da informação
- Organizando a segurança da informação
- Gestão de ativos
- Segurança em recursos humanos
- Segurança física do ambiente
- Gestão das operações e comunicações
- Controle de acesso
- Aquisição, desenvolvimento e manutenção de sistemas de informação
- Gestão de incidentes da segurança da informação

- Gestão da continuidade do negócio
- Conformidade

Falando em Governança de TI, podemos verificar que a ISO 27000 é "totalmente aderente" ao modelo de Governança do COBIT, ou vice-versa. Se quisermos, podemos mapear praticamente todas as seções acima aos processos que o COBIT 4.1 traz. Para fins de exemplo, podemos pegar a seção "Gestão de incidentes da segurança da informação" acima e tratar os incidentes da segurança dentro do processo de gestão de incidentes propostos pelo COBIT 4.1 (DS8) e ITIL (Operação de Serviço: Gestão de Incidentes), mas tratando o incidente da segurança de acordo com o sugerido pela norma ISO 27000. Portanto, caso sua empresa tenha um service desk baseado nas práticas do ITIL, só precisaria incluir mais alguns procedimentos para o tratamento dos incidentes de segurança.

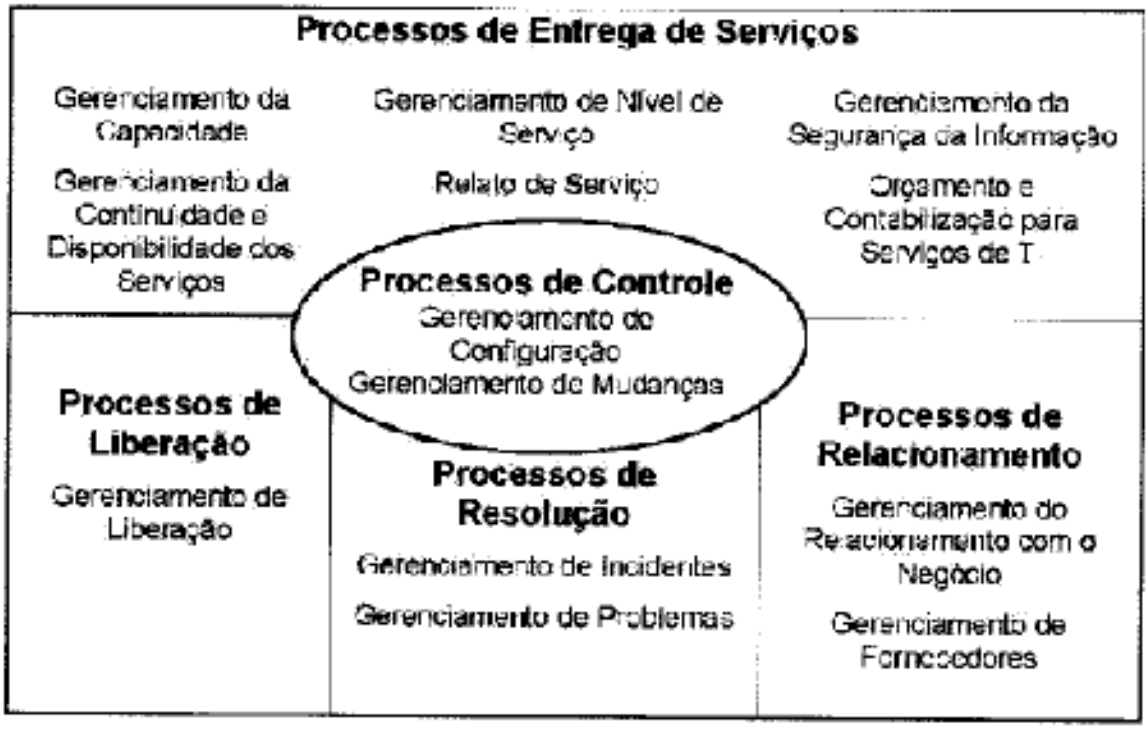
ISO 20.000 – Vale à pena investir?

Segundo uma matéria da ótima revista de TI "InformationWeek" do mês de Janeiro, com a capa: "ISO 20 mil, vale a pena investir para tirar a certificação?", onde a reportagem destaca a obtenção do selo ISO 20000 pela TI do Brasil com um investimento abaixo de 100 mil reais.

Primeiro, vamos nos localizar sobre o assunto. A ISO 20000, segundo a Wikipédia:

> *"É a primeira norma editada pela ISO (International Organization for Standardization) que versa sobre gerenciamento de serviços de TI (Tecnologia da Informação).A ISO 20000 é um conjunto que define as melhores práticas de gerenciamento de serviços de TI. O seu desenvolvimento foi baseado na BS 15000 (British Standard) e tem a intenção de ser completamente compatível com o ITIL (Information Technology Infrastructure Library). A sua primeira edição ocorreu em Dezembro de 2005."*

Esta norma é baseada na versão 2 da ITIL, que é de 2001. Para quem conhece os processos e conceitos da ITIL, facilmente se identifica com ela. Os processos da norma podem ser vistas na figura abaixo:



ISO 20000 – processos

A ISO 20000 é dividida em dois documentos, a Parte 1 – A Especificação e Parte 2 – Código de Práticas.

Parte 1: Especificação

1: Escopo – Requisitos para o provedor de serviços entregar serviços gerenciados com qualidade aceitável.

2: Termos e definições

3: Requisitos para um sistema de gestão

4: Planejamento e implementação do gerenciamento de serviço (PDCA)

5: Planejamento e implementação de serviços novos ou modificados

6: Processo de Entrega de serviço

7: Processos de relacionamento

8: Processos de resolução

9: Processos de Controle

10: Processo de Liberação

Parte 2: Código de Práticas

1: Escopo – Esta parte da ABNT NBR ISO/IEC 20000 fornece orientação para auditores e assiste fornecedores de serviços no planejamento de melhorias dos serviços, ou para serem auditados na ABNT NBR ISO/IEC 20000-1.

2 : Termos e definições

3: O sistema de gestão (Responsabilidades, documentações, desenvolvimento profissional, educação, treinamento)

4: Planejamento e implementação do gerenciamento de serviço (PDCA)

5: Planejamento e implementação de serviços novos ou modificados

6: Processo de Entrega de serviço

7: Processos de relacionamento

8: Processos de resolução

9: Processos de Controle

10: Processo de Liberação

Em relação aos processos da versão 2 da ITIL, podemos notar algumas diferenças: os processos relato de serviço, relacionamento com o negócio e relacionamento com fornecedor. Os processos de “relato do serviço” e “relacionamento com o negócio”, podemos traçar um paralelo na versão 2 da ITIL com atividades dentro do Gerenciamento de Nível de Serviço, como relato do serviço sendo os relatórios reportando os níveis de serviço fornecidos pelo provedor de serviços que são repassados e revisados com os clientes, e o relacionamento com o negócio sendo a gestão do relacionamento com o clientes que é feito no processo de Gestão de Nível de Serviço. O gerenciamento de fornecedor virou um processo dentro da ITILV3, no estágio Desenho do Serviço.

Voltando a reportagem citado no início, a mesma não destaca claramente os benefícios obtidos pelo Banco do Brasil com a obtenção do “selo”. A reportagem menciona somente que diferente do ITIL, com a ISO é reforçado o compromisso da melhoria continuada, devido à

necessidade de se seguir os processos documentados, sendo eles periodicamente auditados interna e externamente para a manutenção do selo. Lembrando que a "perda" do selo é um dano a imagem da empresa. E qual papel da ITIL além de ser o "modelo" onde a ISO 20000 foi baseada? A reportagem cita que o início da preparação aplicou os processos no modelo ITIL. Isso ajudou com certeza a criar uma cultura voltada a gestão de serviços de TI e melhoria contínua, e também facilitou a adequação dos processos para obtenção do selo.

Além de certificar empresas, a ISO 20 mil tem através do EXIN uma prova foundation para certificar profissionais em seus conceitos. Os assuntos da prova e o simulado oficial pode ser encontrado em exin-exams.

Gerenciando Projetos com PMBOK

Atualmente dentro das áreas de TI, fala-se muito em projetos. Quase tudo é um projeto. Por isso, mesmo que não tenhamos contato direto com projetos ou com a gestão deles, é muito importante termos ao menos alguma noção do que é um projeto e de como é estruturado. Segue algumas definições sobre o assunto.

O que é projeto?

Segundo o PMBOK:

> *"Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. Os projetos e as operações diferem, principalmente, no fato de que os projetos são temporários e exclusivos, enquanto as operações são contínuas e repetitivas."*

Resumindo, projeto é o evento que tem início e fim (escopo) bem definidos. Diferente de uma operação, execução de backup, por exemplo, que é uma tarefa diária e não se sabe quando ela não será mais necessária. É algo rotineiro.

O que é o PMBOK?

O Project Management Body of Knowledge (Conjunto de Conhecimentos de Gestão de Projetos) é um conjunto de melhores práticas para Gestão de Projetos, que é mantida pelo PMI(Project Management Institute). Assim como ITIL está para Gestão de Serviços em TI e o COBIT está para Governança de TI, o PMBOK está para gestão de projetos. Existe uma metodologia também bastante conhecida em projetos que é o Prince2.

Como o PMBOK está estruturado?

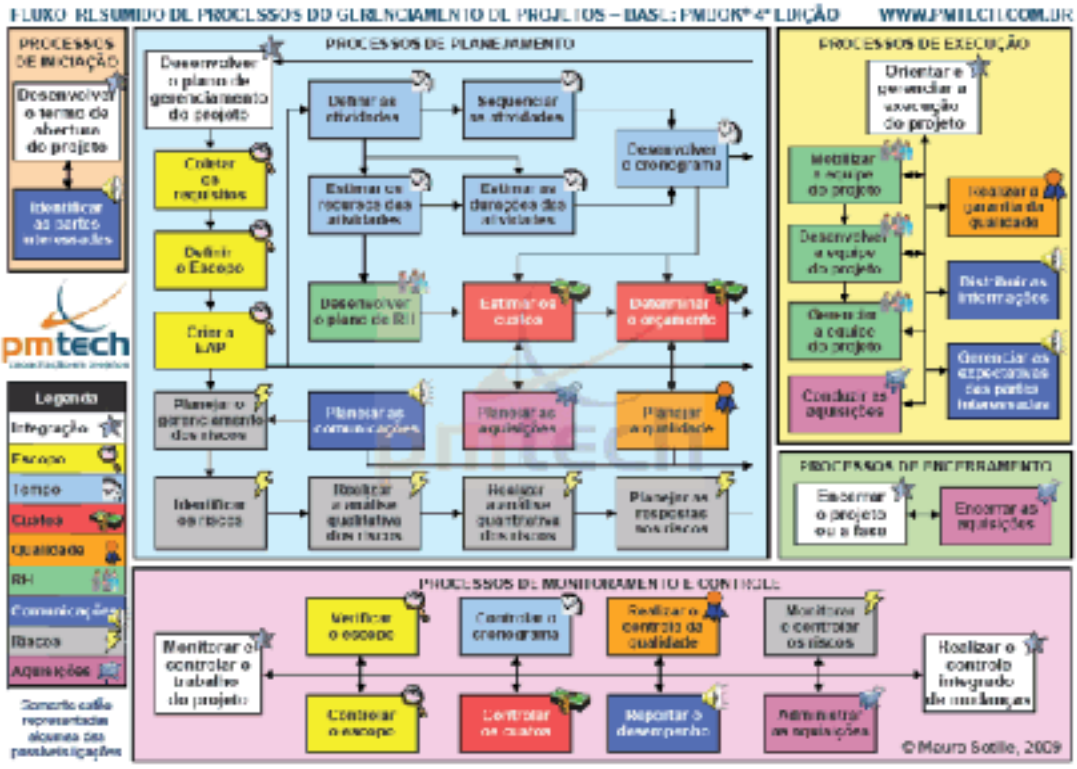
O modelo está estruturado em 9 áreas de conhecimento de projetos, a saber:

- Integração
- Escopo
- Tempo
- Custos
- Qualidade
- Recursos Humanos
- Comunicações
- Riscos
- Aquisições

Estas áreas de conhecimento estão “embutidas” na forma de processos dentro dos grupos de processos do PMBOK. No total são 44 processos. Para quem já estudou ITILv3, é possível comparar estes grupos de processos com os estágios do ciclo de vida (estratégia, desenho e etc), que são:

- Iniciação
- Planejamento
- Execução
- Monitoramento e controle
- Encerramento

Na figura a seguir estão os processos pertencentes a cada grupo do PMBOK:



O principal “ator” do Gerenciamento de Projetos é o Gerente de Projetos, que é a pessoa que tem os conhecimentos na gestão de projetos e tem responsabilidade de conduzir os projetos dentro do custo, prazo e qualidade necessários. Os Outros A ”atores” de um projeto são o sponsor, a pessoa que efetivamente paga pelo projeto, e os stakeholders, que são todas as pessoas beneficiadas ou não pelo projeto ou que de alguma maneira são afetadas. As pessoas que efetivamente realizam as atividades são comumente chamados de recursos”.

Quais as certificações existentes?

Atualmente o PMBOK tem certificação somente para profissionais, que são o PMP para gerente de projetos e CAPM que é para gerentes de projetos iniciantes ou pessoas envolvidas no projeto. Para ser um profissional certificado, além do exame é necessário comprovar um número de horas em gestão de projetos.

Quais os benefícios em gerenciar projetos?

Segundo estudo do *Center for Business Practices (2001)*, foi identificado melhoras em: atendimento a prazos, qualidade, satisfação dos clientes, melhoria do time-to-market, custo, produtividade entre outros benefícios.

Tópicos relacionados

Com a evolução da gestão de projetos, outras ferramentas e técnicas vêm ganhando força, já que as empresas gerenciam muitas vezes dezenas de projetos ao mesmo tempo, e muitas vezes relacionados entre si. Hoje fala-se muito em portfólio de projetos, programas de projetos e PMO.

Auditoria de TI – mal necessário?

Vamos iniciar com uma ilustração:

Era para ser um dia normal, mas o dia começou cinza e todos estão tensos. O chefe chegou extremamente preocupado e logo de manhã reúne a equipe e diz: “Leiam os procedimentos e registrem o que está faltando, pois amanhã temos a auditoria externa. Se perdermos o selo da ISO cabeças vão rolar!”

Alguma semelhança com algo que você já presenciou, viu ou ouviu?

Empresas e profissionais buscam mostrar ao mercado que estão aptos a atenderem seus clientes (internos e externos) dentro de padrões de qualidade. Muitas vezes esta busca por qualificação e certificação é um instrumento utilizado mais para marketing pessoal/empresarial do que garantir que as entregas são feitas com a qualidade esperada pelo cliente, mas acredito que esta seja a minoria.

Quando falamos em Governança de TI, um dos objetivos de se implementar certificações/auditorias, é a busca de transparência da área de TI perante seus stakeholders (a organização, clientes e principalmente a alta administração). A TI é um ativo estratégico que representa um risco dentro da organização, já que suporta de alguma forma praticamente todos os processos de negócio, e por isso precisa ser mitigado. Alguns regulamentos como a SOX (http://www.governancadeti.com/2010/08/governanca-de-ti-lei-sarbanes-oxley-e-a-ti/) aumentam ainda mais esta necessidade de transparência, pois os gestores do negócio são responsabilizados em causa de fraudes e/ou por desobediência a estas leis. Neste contexto, ao contrário do cenário que abordamos no início do post, a auditoria de TI precisa ser encarada como algo que agrega maior valor a TI, e não como algo que serve para revelar as falhas das pessoas e puni-las. Um relato interessante sobre os benefícios de auditorias externas pode ser encontrado no site tiespecialistas (http://www.tiespecialistas.com.br/2011/02/a-importancia-de-uma-auditoria-de-sistemas-independente/).

Nós profissionais de TI precisamos nos colocar no lugar de quem está à frente do negócio. Por melhor que seja a equipe de TI, como ter certeza que de fato que a TI está alinhada com a empresa e mitigando os riscos? Nós profissionais de TI sabemos na prática aos riscos que estamos sujeitos e o impacto que isto pode causar para o negócio, tanto em imagem quanto financeiro.

Alguns exemplos de itens simples que geram grande impacto para o negócio se não forem bem gerenciados: backup, processos de gestão de serviços, segurança da informação, sistemas e etc. Isto para não entrar no mérito das empresas que necessitam de auditoria externa por obrigações legais. Acredito que este exame de conformidade que a auditoria traz, comprova que a TI está no

caminho certo, ou então aponta o que está errado e precisa ser corrigido. Vejo que é uma forma do negócio compartilhar de fato as responsabilidades da TI e seus riscos.

O COBIT é uma ferramenta muito utilizada em auditorias de TI. Ele permite uma avaliação padronizada para fundamentar a opinião do auditor sobre a TI da organização e permite apresentar recomendações à administração sobre melhoria dos controles internos.

A conclusão que chegamos com esta reflexão é que a auditoria de TI é um "bem necessário", que traz benefícios para todos os stakeholders de TI, desde clientes, passando pela alta administração e principalmente para a própria TI.

Bibliografia

http://itweb.com.br/voce-informa/o-que-e-governanca-de-ti/

http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx

http://www.governancadeti.com

http://www.administradores.com.br

http://www.efagundes.com/artigos/Sox_e_o_impacto_em_TI.htm

http://www3.itsmcampus.com/isaca/error.aspx?aspxerrorpath=/isaca/Catalog/catalog_details.aspx

http://pt.wikipedia.org/wiki/CMMI

http://cio.uol.com.br/gestao/2009/09/14/especialista-do-mit-so-38-das-empresas-brasileiras-tem-governanca-de-ti/

http://www.aghatha.com.br

http://www.mor-officialsite.com/home/home.asp

http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx

http://www.exin-exams.com/exams/exam-program/iso-iec-20000/is20f.aspx