UNIVERSIDADE ESTADUAL DE LONDRINA

Trabalho de Conclusão de Curso

Mateus de Paula Marques

Governança de TIC utilizando ITIL®V3 e COBIT®

Londrina

2010

Agradecimentos

Aos meus pais, pela oportunidade de realizar este curso.
Ao professor Mario, por me aceitar como orientando.
Aos meus amigos Natália e Ricardo (Dizus), pela ajuda que me proporcionaram durante a revisão deste trabalho.
Aos integrantes do Grupo de Estudos de Redes, pelo trabalho desempenhado ao longo deste ano.
A todos os integrantes do curso de Ciência da Computação.

"Os meus gametas se agrupam no meu som."

Zé Ramalho

Resumo

A crescente adoção das melhores práticas de Tecnologia da Informação e Comunicação (TIC) nas organizações é resultado da necessidade de gerenciar sua qualidade e confiabilidade nos negócios, a fim de responder ao grande número de requisitos regulatórios e contratuais existentes. Neste contexto, surgiram as práticas de Governança e Gerenciamento de Serviços de TIC, que são abordadas neste trabalho através de um alinhamento realizado entre os *frameworks* ITIL® e COBIT®. O primeiro, apresenta um conjunto de melhores práticas para o Gerenciamento de Serviços de TIC, e o segundo, para a Governança de TIC. Ambos são as ferramentas mundialmente mais aceitas para a aplicação destas técnicas e, se forem corretamente utilizadas, podem fazer com que a TIC deixe de ser apenas um setor de apoio para a organização, tornando-se um ativo de grande valor estatégico.

A partir disso, este trabalho tem o objetivo de realizar um alinhamento entre esses dois *frameworks*, objetivando apontar a eficácia do ITIL® em atender os requisitos de processo do COBIT®, no que tange o Gerenciamento de Serviços de TIC.

Palavras-chaves: TIC, ITIL®, COBIT®, Governança de TIC, Gerenciamento de Serviços de TIC.

Abstract

The growing adoption of Information Technology and Communication (ITC) best pratices on the organizations has been caused by the need to manage its quality and reliability in business, responding to the great number of contratual and regulamentory requirements. At this context, the ITC Governance and Service Management pratices arise and are addressed by this work through an proposed aligniment of the ITIL® and COBIT® frameworks. The first one, brings up a set of best pratices for the ITC Service Management, while the second, a set of control objectives for ITC Governance. Both are the worldwide most accepted tools to the application of this pratices, and if correctly set, they can provide the ITC as a strategic asset for the organization.

So, this work looks to present an aligniment between both *frameworks*, in order to show precisely the effectiveness of the ITIL® in regard with the COBIT's® requirements.

Keywords: ITC, ITIL®, COBIT®, ITC Governance, ITC Service Management.

Sumário

Lista de Siglas e Abreviaturas

AI *Acquire and Implement*

AM *Avaliability Management*

BIA *Business Impact Assessment*

BSC *Balanced Scorecard*

CAB *Change Advisory Board*

CICA *Canadian Istitute of Chartered Accountants*

CM *Crisis Management*

CMDB *Configuration Management Database*

CMIS *Capacity Management Information System*

CMMI-DEV *Capability Maturity Model Integration for Development*

COBIT *Control Objectives for IT and Related Technologies*

COSO *Comitee of Sponsoring Organizations of the treadway Comissions*

CSF *Critical Success Factor*

DML *Definitive Media Library*

DOS *Denial of Service*

DS *Deliver and Support*

DTI *Departament of Trade and Industry*

ECAB *Emergency Change Advisory Board*

ISACA *Information Systems Audit and Control Association*

ISM *Information Security Management*

ISMS *Information Security Management System*

ISO *International Organization for Standardization*

ITCG *Information Technology Control Guidelines*

ITGI *Information Technology Governance Institute*

ITIL *Information Technology Infraestructure Library*

ITSCM *Information Technology Service Continuity Management*

KPI *Key Performance Indicator*

ME *Monitor and Evaluate*

MTBF *Mean Time Between Failures*

MTRS *Mean Time to Restore Service*

MTBSI *Mean Time Between Service Incidents*

NIST *National Institute of Standards and Technology*

OECD *Organization for Economic Cooperation and Development*

OLA *Operational Level Agreement*

PDCA *Plan, Do, Chek and Act*

PMBOK *Project Management Body of Knowledge*

PO *Plan and Organize*

RDM *Release and Deployment Management*

RFC *Request For Change*

ROI *Return Over Investiment*

SCC *Security Code of Conduct*

SCDB *Supplier Contract Database*

SCM *Service Catalogue Management*

SIP *Service Improvement Plan*

SKMS *Service Knowledge Management System*

SLA *Service Level Agreement*

SLM *Service Level Management*

SLR *Service Level Requirement*

SLT *Service Level Target*

SM *Supplier Management*

SMART *Specifica, Measurable, Achievable, Results Oriented and Time Specific*

SOR *Statement of Requirements*

TCO *Total Cost of Ownership*

TIC Tecnologia da Informação e Comunicação

UC *Underpinning Contract*

VBF *Vital Business Function*

VOI *Value of Investiment*

Lista de Figuras

Lista de Tabelas

Introdução

No setor corporativo, vem se tornando cada vez mais frequente o reconhecimento de que a informação é o recurso estratégico mais importante que qualquer tipo de organização deve gerenciar. A chave para a coleção, análise, produção e distribuição da informação dentro de uma organização é a qualidade dos serviços de Tecnologia da Informação e Comunicação (TIC) que suportam os negócios. É essencial reconhecer que os serviços de TIC são ativos estratégicos e organizacionais muito importantes, de forma que as organizações devem investir níveis de recursos apropriados no suporte, na entrega e no gerenciamento desses serviços, e principalmente nas tecnologias que os suportam. No entanto, estes conceitos são, de certa forma, negligenciados ou apenas superficialmente tratados dentro de muitas organizações [6].

Os principais desafios dos Gerentes de Negócios e de TIC atualmente são: o planejamento estratégico do negócio de TIC, alinhar o setor de TIC ao setor de negócios (existe uma grande lacuna no que tange à comunicação dessas partes), implementar uma técnica para obter melhoria contínua nos serviços prestados pela organização, mensurar a efetividade e a eficiência da organização, otimizar os Custos Totais de Propriedade[1] (TCO - *Total Cost of Ownership*), dentre outros [19]. Esses desafios são importantes para coordenar e trabalhar em parceria com o negócio, e também para entregar alta qualidade de serviços de TIC. Tal objetivo pode ser alcançado quando se adota uma característica orientada ao negócio e ao cliente, para entregar melhores serviços com menores custos.

Neste cenário, a Governança de TIC surge com o objetivo de resolver os problemas do setor, ligando os seus desafios com uma estrutura de controle e, desta forma, determinando como eles podem ser melhor gerenciados. Essa estrutura define as razões pelas quais governar é necessário, e o que é preciso realizar para obter efetividade [2].

O Gerenciamento de Serviços originou-se de empresas de serviços tradicionais, como por exemplo companhias aéreas, hotéis, empresas de telefonia, etc. A adoção de características orientadas a serviço pelas organizações de TIC contribui para um aumento significativo desta prática. A popularidade da terceirização contribuiu para o aumento do número de organizações prestadoras de serviço. Isso, por sua vez, fortaleceu ainda mais a prática do Gerenciamento de Serviços, e ao mesmo tempo, impôs maiores desafios a ele [8].

Neste trabalho serão estudados os *frameworks* COBIT® e ITIL® utilizados para Governança

[1] É uma estimativa financeira com o objetivo de avaliar os custos diretos e indiretos relacionados à compra de um produto.

e Gerenciamento de Serviços de TIC, respectivamente. No capítulo 2 serão apresentados conceitos básicos sobre Governança de TIC, o seu funcionamento e, finalmente, como ela se relaciona com a Governança Corporativa. No capítulo 3 e 4 são detalhados os processos dos *frameworks* COBIT® e ITIL®, respectivamente. E por fim, no capítulo 5 será apresentado um alinhamento entre os processos do ITIL® e do COBIT®, uma visão precisa para a Governaça de TIC no que tange o Gerenciamento de Serviços, relacionando a superficialidade dos processos do COBIT®, com o aprofundamento dos processos do ITIL®.

1 Governança de TIC

Segundo o Instituto de Governança de Tecnologia da Informação (ITGI - *Information Technology Governance Institute*), a Governança de TIC é *"a capacidade da organização em controlar o planejamento e a implementação da estratégia de TIC, e dar direção de novos rumos e investimentos a fim de atingir vantagem competitiva para a companhia"* [3].

A partir disso, podemos interpretá-la como uma atividade de nível gerencial, que clarifica a autoridade para tomadas de decisão, determina a responsabilidade de ações e finalmente, facilita na medição do desempenho.

Desta forma, considerando a importância da TIC para atividades do setor, a Governança de TIC não pode ser tratada em um escopo diferente da Governança Corporativa.

1.1 Governança Corporativa

A Governança Corporativa é o conjunto de processos, costumes, políticas e leis que ditam a maneira na qual uma organização é controlada. Ela também inclui os relacionamentos entre os vários interessados envolvidos no negócio, e os objetivos para os quais a organização é governada [20].

Um conceito importante deste tema é garantir a responsabilidade de indivíduos na organização. Um assunto relacionado foca no impacto que um sistema de Governança Corporativa pode causar na eficiência econômica da organização, com grande ênfase no bem estar dos interessados no negócio.

Por fim, a Governança Corporativa deve cuidar de questões como assegurar o *Return Over Investiment* (ROI), controlar os gestores, e finalmente, garantir que o dinheiro investido não seja expropriado ou aplicado a projetos que estejam fora dos objetivos da organização.

1.2 Governança Corporativa e Governança de TIC

Tendo em vista que atualmente a TIC está envolvida em praticamente todos os processos de negócios que envolvam a manipulação de informações, a Governança de TIC e a Gorvernança Corporativa não podem ser tratadas em escopos separados. Isso torna-se evidente através da análise de vários fatores, como segue:

- A Governança de TIC integra e institucionaliza melhores formas de planejar e organizar, adquirir e implementar, entregar e suportar, e finalmente, monitorar e avaliar a performance de TIC. [3]

- A Governança Corporativa é o sistema pelo qual as entidades são dirigidas e controladas, assim, ela dirige e configura a Governança de TIC. Ao mesmo tempo, a Governança de TIC fornece dados críticos para planos estratégicos, influenciando nas opções por oportunidades estratégicas delimitadas pela organização. [3]

  Vale ressaltar o fato de que, atualmente, a Governança Corporativa é totalmente impraticável sem a Governança de TIC. Questões como a garantia do ROI, a integridade de capital e, principalmente, o controle de gestão não podem ser tratadas sem que hajam medições confiáveis. Muitos autores ainda reforçam o fato de que é impossível governar o que não se pode medir. A confiabilidade dessas medições, por sua vez, depende integralmente da qualidade dos produtos de TIC (*software, hardware,* recursos humanos) responsáveis por elas. A partir disso é totalmente pertinente concluir que o Controle, uma das propriedades mais importantes da Governança Corporativa, não é garantido sem que exista uma sólida Governança de TIC.

Para atender às necessidades do setor de negócios, a Governança de TIC define estruturas de controle a fim de nortear suas atividades. São elas:

- Foco no Negócio: *"Prover foco no negócio para permitir o alinhamento entre os objetivos de negócio e de TIC"*. [3]

- Orientação a Processo: *"Estabelecer orientação a processos para definir o escopo e a extensão da cobertura, com uma estrutura definida que permita fácil navegação dos conteúdos"*. [3]

- Aceitabilidade Geral: *"Ser geralmente aceitas por serem coerentes com as boas práticas e normas independente de tecnologias específicas"*. [3]

- Linguagem Comum: *"Fornecer uma linguagem comum com um conjunto de termos e definições que são geralmente compreensíveis por todos os stakeholders*[1]*"*. [3]
- Requerimentos Regulatórios: *"Ajudam a satisfazer os requisitos regulatórios por serem coerentes com as normas geralmente aceitas de Governança Corporativa, e com os controles de TIC esperados pelas autoridades reguladoras e auditores externos"*. [3]

Esses fatores sob uma gerência provida das devidas competências comportamentais, são completamente capazes de garantir as questões apontadas pela Governança Corporativa [2]. Esta, por sua vez, possui o *Comittee of Sponsoring Organizations of the Treadway Commission's* (COSO) como estrutura de controle amplamente aceita para governar e gerenciar riscos [20], ja a Governança de TIC possui o *Control Objectives for Information and related Technology"* (COBIT®) como estrutura de controle amplamente aceita para suas atividades [18].

1.3 A Governança de TIC e as suas áreas de atuação

Segundo o ITGI, a Governança de TIC a fim de garantir que o setor obtenha os resultados almejados pela Governança Corporativa, atua em 6 grandes áreas, devido ao grande número de diferentes aplicações relacionadas, são elas: [4]

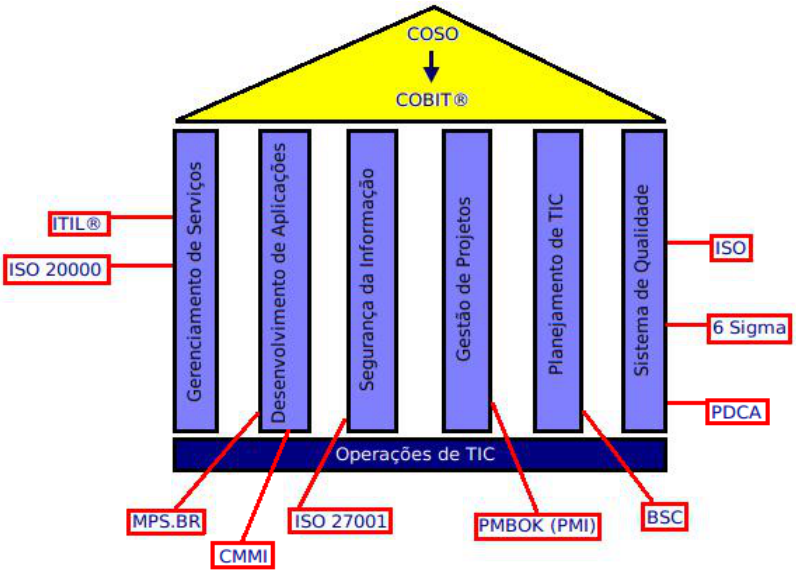

Figura 1.1: Áreas de atuação da Governança de TIC.

[1]Refere-se a toda e qualquer parte interessada que deve estar de acordo com as práticas de governança executadas pela empresa. [18]

- **Gerenciamento de Serviços:**

  O Gerenciamento de Serviços é um conjunto de capacidades organizacionais especializadas em prover valor aos clientes na forma de serviços. Essas habilidades tomam a forma de funções e processos para gerenciar serviços sob um ciclo de vida, com especializações em estratégia, desenho, transição, operação e melhoria contínua. As habilidades representam a capacidade e a competência da organização em desempenhar suas atividades. O ato de transformar recursos em serviços valiosos está no núcleo do gerenciamento de serviços, e sem essas habilidades, uma organização de serviços é meramente um conjunto de recursos que tem baixo valor para os clientes.

  Assim, esta área objetiva utilizar um conjunto de melhores práticas para o Gerenciamento de Serviços, a fim de obter maior utilidade e garantia nos serviços prestados. O ITIL® é o framework mais amplamente adotado, e a ISO/IEC 20000 é o padrão formal e universal para auditoria e certificação de organizações fazem uso do Gerenciamento de Serviço. [8]

- **Desenvolvimento de Aplicações:**

  O Desenvolvimento de Aplicações pode ser definido como o desenvolvimento de *software* a partir de um projeto estruturado. Através do *Capability Maturity Model Integration for Development* (CMMI-DEV®), esta área de atuação objetiva obter melhoria de qualidade no desenvolvimento de software.

  O CMMI-DEV® consiste em um conjunto de melhores práticas que endereçam atividades de desenvolvimento aplicadas a produtos e serviços. Ele encaminha práticas que cobrem o ciclo de vida dos produtos desde a sua concepção até a entrega e manutenção. [5]

- **Segurança da Informação:**

  Esta área de interesse tem a função de manter o valor dos dados para a organização, garantindo a confiabilidade, integridade e disponibilidade destes. A ISO/IEC 27001 é o padrão internacional que certifica as organizações que implementam esta atividade.

  O padrão ISO/IEC 27001 é uma especificação para Sistemas de Gerenciamento da Segurança da Informação (ISMS), que tem como principal objetivo fornecer um modelo para gerenciar efetivamente a segurança das informações da organização, uma abordagem que em muitos casos, pode ser considerada a partir de uma decisão estratégica. Além disso, implementar um ISMS é uma atividade que deve levar em consideração fatores como as necessidades, objetivos, processos empregados, requisitos de segurança e até o tamanho da organização. [1]

  Por fim, visando manter os níveis atingidos, este padrão aplica o modelo PDCA (seção 3.4.18) para estruturar os processos, e assim refletir aos princípios estabelecidos no *Organization for Economic Co-operation and Development* (OECD).

- **Gestão de Projetos:**

  A Gestão de Projetos visa aplicar um conjunto de boas práticas às atividades da organização a fim de atender as necessidades dos *stakeholders* com relação aos projetos. Esses projetos, por sua vez, devem ser subdivididos em várias fases, a fim de proporcionar uma maneira mais simples de controle, além de facilitar o desenvolvimento de atividades em conjunto com as operações que estão ocorrendo na organização.

  Desta forma, esta área de atuação deve manter foco em planejar, organizar, assegurar e gerenciar recursos a fim de alcançar com sucesso os objetivos de determinados projetos. O *Project Management Body of Knowledge* (PMBOK®) é o conjunto de boas práticas mais aceito para este fim. [10]

- **Planejamento de TIC:**

  O Planejamento de TIC, ou Planejamento Estratégico de TIC deve proporcionar melhores direcionamentos nos investimentos da área, redução de custos, melhoria de produtividade e qualidade na adoção de soluções de TI, e finalmente, agilidade e melhor tempo de resposta às mudanças no contexto onde está inserida a organização, tudo isso com o objetivo de aumentar a satisfação dos usuários (clientes) de TIC. Sendo assim, este é considerado uma disciplina que preocupa-se em manter o planejamento de processos para investimentos e tomadas de decisões, para que estes tornem-se mais rápidos, flexíveis e completamente alinhados. O *Balanced Scorecard* (BSC) é a metodologia de medição e gestão de desempenho mais utilizada para essas tarefas.

  O BSC é um sistema de planejamento desenvolvido com o objetivo de adicionar medidas de performance fora do âmbito financeiro às métricas financeiras tradicionais, a fim de fornecer aos executivos uma visão balanceada em relação ao desempenho da organização. Quanto à sua utilização, ele é aplicado a funções que abrangem desde a simples medição de performance até os complexos sistemas de planejamento estratégico. Por fim, o BSC apresenta um *framework* que além de fornecer medidas de performance, ajuda os planejadores a identificar o que deve ser feito e medido, fazendo com que os executivos realizem suas estratégias com sucesso. [7]

- **Sistema de Qualidade:** Objetiva garantir a qualidade dos serviços/produtos da organização. A ISO/IEC 9000 certifica as organizações que implementam com efetividade o seu conjunto de requisitos. O *Six Sigma* é o conjunto de práticas mais utilizado como estratégia gerencial neste contexto, a fim de promover mudanças nas organizações objetivando a melhoria contínua.

  O *Six Sigma* tem como princípio reduzir continuamente a variação dos processos, visando a eliminação de defeitos ou falhas nos resultados (produtos ou serviços) obtidos. Sendo assim, para manter sua ênfase no controle de qualidade bem como na análise e solução de

problemas, ele faz uso intenso do ciclo PDCA (ou ciclo de Deming), que tem foco direto na melhoria contínua. [9]

O Ciclo de Deming, por sua vez, é aplicado em sistemas de gestão com o objetivo de atingir resultados específicos, mantendo e melhorando metas especificadas. Este mantenimento é extremamente importante para que a organização não *"volte no tempo"*, com relação às melhorias obtidas.

Por fim, no que tange os Sistemas de Qualidade, a ISO é o conjunto de normas e técnicas que estabelecem um modelo de gestão de qualidade alcançável por qualquer tipo de organização, independentemente do ramo em que ela se encontre. Esta família de normas estabelece requisitos que tem como objetivo final oferecer maior produtividade e credibilidade às organizações perante o mercado.

2 *COBIT® 4.1*

O framework COBIT® foi criado na década de 90 pelo *Information System Audit and Control Association* (ISACA®), possui uma estrutura baseada em indicadores de performance a fim de monitorar o quanto o setor de TIC está agregando valores ao negócio. Ele foca basicamente em três níveis distintos. Primeiramente os gerentes de TIC, que possuem a responsabilidade de avaliar riscos e controlar investimentos; os usuários, que através de suas competências comportamentais e técnicas, devem assegurar a qualidade dos serviços prestados a clientes, sejam eles internos ou externos; e finalmente os auditores, cuja função é avaliar o trabalho do setor de TIC e trabalhar no controle interno da organização. [4]

Existe um grande número de modelos para controle apenas de TIC, como por exemplo:

- **SCC** (*Security Code of Conduct* - Código de Segurança de Conduta) do **DTI** (*Departament of Trade and Industry* - Departamento de Comércio e Indústria) na Inglaterra.
- **ITCG** (*Information Tecnology Control Guidelines* - Diretrizes para o Controle da Tecnologia da Informação) do **CICA** (*Canadian Institute of Chartered Accountants* - Instituto Canadense de Contabilidade) no Canada.
- **Manual da Segurança** (*Security Handbook*) do **NIST** (*National Institute of Standards and Technology* - Instituto Nacional de Segurança e Tecnologia) nos EUA.

No entanto, estes modelos de controle são muito específicos, e não fornecem um método usável e compreensível sobre TIC, ou seja, não há suporte de processos de negócio. O propósito do COBIT® é criar uma ponte para eliminar este *gap*, fornecendo um framework que é especificamente ligado aos objetivos de negócio, enquanto foca o setor de TIC. [2]

Desta forma, a missão do COBIT® dentro de uma organização é pesquisar, desenvolver, publicar e promover um framework de Governança de TIC orientado ao negócio, baseado em controle, dirigido por métricas e internacionalmente aceito que garanta que o setor de TIC obtenha os resultados esperados pela Governança Corporativa. [4]

2.1 Os Domínios do COBIT®

O COBIT® define suas atividades em trinta e quatro processos divididos em quatro domínios que mapeiam as áreas de responsabilidade do setor de TIC, são eles:

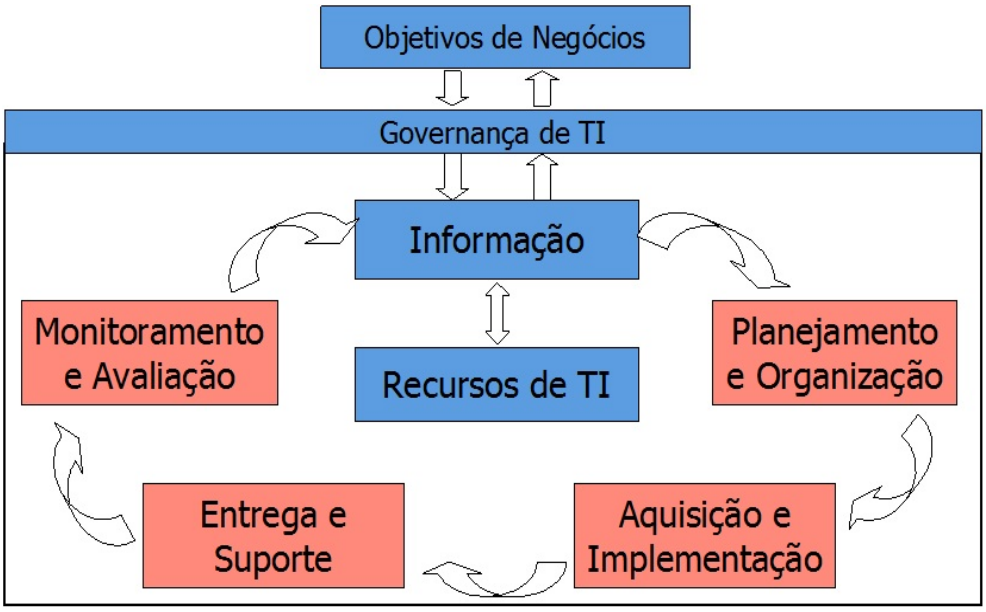

Figura 2.1: Os Domínios do COBIT®.

- **Planejamento e Organização:**

  Este domínio deve cuidar dos assuntos do setor de uma perspectiva estratégica, avaliando oportunidades nas quais o setor de TIC pode obter maior desempenho, e assim ajudar para que a organização alcance seus objetivos. Além disso, questões como gerência de riscos, investimentos, recursos humanos e qualidade devem ser tratados neste domínio, a fim de concretizar as metas por ele estabelecidas. [4]

- **Aquisição e Implementação:**

  Este domínio deve integrar todas as soluções de TIC no processo de negócio, a fim de desenvolver as estratégias definidas pelo setor. Para isso, essas soluções devem ser desenvolvidas ou adquiridas, e por fim implementadas no ambiente. Toda e qualquer mudança realizada no ambiente também deve ser tratada por este domínio, uma vez que essas mudanças devem ser desenvolvidas a partir da mesma perspectiva de desenvolvimento utilizada novas soluções. [4]

- **Entrega e Suporte:**

  Este domínio deve abordar todos os aspectos relativos a entrega e suporte de soluções de TIC, além de analisar informações geradas por aplicações, a fim de garantir que as soluções estejam oferecendo a segurança, a performance e a continuidade necessárias. [4]

- **Monitoração e Avaliação:**

  Este domínio deve consolidar a governança de TIC dentro do setor, através de técnicas de monitoramento e avaliação. É nele que todas as informações necessárias são colocadas em uma linguagem comum, para que a governança corporativa possa utilizar o setor de TIC como um ativo estratégico da organização. [4]

Os processos são os objetivos de controle que provêem um conjunto de alto nível de requerimento a ser considerado pelo gerenciamento. Os Controles por sua vez, são definidos como políticas, procedimentos, práticas e estruturas organizacionais designadas a garantir que os objetivos de negócio serão alcançados e que eventos indesejáveis serão evitados ou detectados e corrigidos.

A estrutura de controle do COBIT® prove uma referência em modelo operacional e linguagem comum para toda a TIC envolvida com o negócio, medindo e monitorando o desempenho e efetivamente estabelecendo uma comunicação eficiente com os provedores de serviços e integrando as melhores práticas de gerenciamento, levando a responsabilidade e a prestação de contas sobre os riscos e objetivos envolvidos.

2.2 Os Processos do COBIT®

A divisão dos processos do COBIT® é realizada como segue:

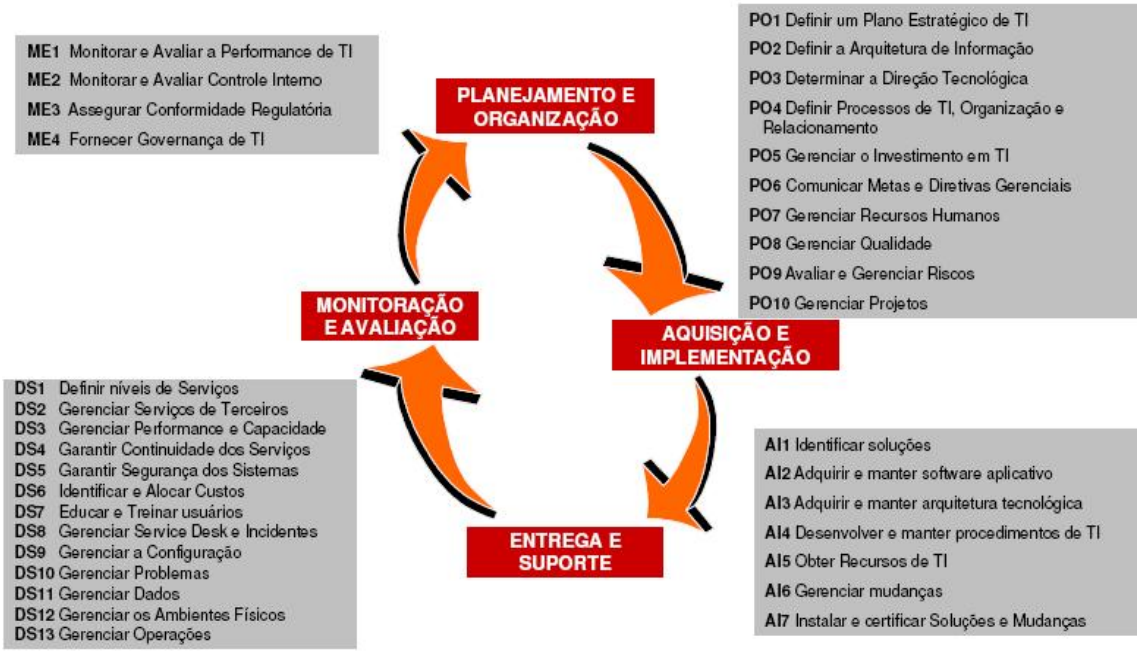

Figura 2.2: Os processos do COBIT® divididos entre os quatro domínios.

Neste capítulo serão apresentados os processos do COBIT®, bem como os seus objetivos de controle.

2.3 Planejamento e Organização

Os processos deste domínio ajudam a identificar maneiras nas quais o setor de TIC pode contribuir para o alcance dos objetivos do negócio, o alinhamento do setor com a estratégia da empresa, a compreensão do pessoal da organização sobre os objetivos do setor e a identificação e gerenciamento dos riscos relacionados ao setor. [3]

2.3.1 Objetivos de Controle

1. **A TIC como parte dos Planos de Curto e Longo Prazo da Organização**

   A alta gerência é responsável por desenvolver e implementar Planos de Curto e Longo Prazo a fim de preencher os objetivos e as missões da organização. Neste contexto, ela deve certificar que as características do setor de TIC bem como as oportunidades são adequadamente avaliadas e refletidas nos planos da organização. Esses planos devem ser

desenvolvidos para ajudar a certificar que o uso dos ativos do setor está de acordo com as estratégias da organização. [2]

2. **Plano de TIC de Longo Prazo**

   Os chefes do Gerenciamento de TIC e dos Processos de Negócio são responsáveis por desenvolver regularmente os Planos de TIC de Longo Prazo suportando a busca pelos objetivos almejados pela organização. A abordagem do planejamento deve incluir mecanismos para solicitar determinadas informações de *stakeholders* internos e externos relacionados aos planos estratégicos de TIC. Assim, o gerenciamento deve implementar processos de planejamento de longo prazo, adotar uma abordagem estruturada e definir uma estrutura de planejamento padrão. [2]

3. **Planejamento de TIC de Longo Prazo - Abordagem e Estrutura**

   Os chefes do Gerenciamento de TIC e dos Processos de Negócio devem estabelecer e aplicar uma abordagem estruturada envolvendo os Processos de Planejamento de Longo Prazo. Isso deve resultar em um plano de alta qualidade que cobre todas as questões básicas como o que, quem, como, quando e por que de cada atividade. O processo de planejamento de TIC deve levar em consideração os resultados da avaliação de riscos. Aspectos que precisam ser considerados e adequadamente encaminhados durante o processo de planejamento incluem o modelo organizacional e as mudanças a ele realizadas, distribuição geográfica, evolução tecnológica, custos, requerimentos legais, requerimentos de terceiros no mercado, etc. Os benefícios das escolhas realizadas devem ser claramente identificados. Os planejamentos de curto e longo prazo do setor de TIC devem incorporar *Key Performance Indicators* (KPIs[1]), e o plano deve referir-se a outros planos, tais como o Plano de Qualidade da Organização e o Plano de Gerenciamento de Risco da Informação. [2]

4. **Mudanças nos Planos de TIC de Longo Prazo**

   Os chefes do Gerenciamento de TIC e dos Processos de Negócio devem certificar que um processo está em posição de modificar o Plano de TIC de Longo Prazo de maneira precisa a fim de acomodar as mudanças no Plano de Longo Prazo da Organização e nas mudanças das condições de TIC. O Gerenciamento deve estabelecer uma política requerendo que os planos de TIC sejam desenvolvidos e mantidos. [2]

5. **Planejamento de Curto Prazo para a Função de TIC**

   Os chefes do Gerenciamento de TIC e dos Processos de Negócio devem certificar que o plano de longo prazo do setor esteja regularmente traduzido em planos de curto prazo. Estes, por sua vez, devem certificar que recursos apropriados de funções de TIC sejam

[1] Os KPIs (Indicadores-Chave de Desempenho) são métricas utilizadas para medir o desempenho de processos e soluções. [13]

alocados de uma forma consistente com o plano de longo prazo. Os planos de curto prazo devem ser reavaliados periodicamente e alterados conforme necessário em resposta as mudanças de negócio e às condições de TIC. Os estudos de viabilidade de performance devem certificar que a execução dos planos de curto prazo seja adequadamente iniciada. [2]

6. **Comunicação de Planos de TIC**

   O Gerenciamento deve certificar que os planos de TIC sejam apresentados aos donos dos processos de negócio, bem como às outras partes relevantes de toda a organização. [2]

7. **Monitoramento e Avaliação dos Planos de TIC**

   O Gerenciamento deve estabelecer processos a fim de solicitar *feedback* dos responsáveis pelos processos de negócio com relação à qualidade e utilidade dos planos. O *feedback* obtido deve ser avaliado e considerado nos planejamentos futuros. [2]

8. **Avaliação dos Sistemas Existentes**

   Antes de desenvolver ou mudar o plano estratégico de longo prazo, o Gerenciamento de TIC deve avaliar os sistemas de informação existentes com relação ao grau de automação de negócio, funcionalidade, estabilidade, complexidade, custo, forças e fraquezas a fim de determinar o quanto esses sistemas suportam os requerimentos de negócio da organização. [2]

2.3.2 PO1 - Definir um Plano Estratégico de TIC

Este processo deve cuidar para que os *stakeholders* tenham total compreensão com relação as oportunidades e limitações do setor, uma vez que eles, juntamente com a função de TIC, são os responsáveis pelo sucesso dos projetos da organização. Além disso, dentro do escopo do plano estratégico está a avaliação da performance e a desmistificação dos investimentos necessários ao setor. O Gerenciamento de Portfólio e do Gerenciamento do Valor de TIC são atividades extremamente importantes para a realização dessas tarefas. Por fim, a estratégia de negócio deve ser refletida nos portifolios e extendida pelos planos de ação e de tarefas, ambos compreendidos e aceitos pelo negócio e pela TIC. [4]

2.3.3 PO2 - Definir a Arquitetura da Informação

Este processo visa melhorar a qualidade das tomadas de decisão, garantindo a confiabilidade das informações apresentadas. Isto é possível quando se gerencia o conhecimento do serviço, habilitando assim o racionamento de recursos de sistemas de informação, a fim de obedecer as estratégias do negócio. Este processo também requisita o aumento da

responsabilização pela segurança dos dados, bem como o controle da informação compartilhada através de aplicações. [4]

2.3.4 PO3 - Determinar a Direção Tecnológica

Este processo visa proporcionar uma visão real relacionada à capacidade tecnológica em termos de soluções, através de um plano de infra-estrutura tecnológica. Este plano deve ser regularmente atualizado, habilitando assim a economia de escala[2], e melhorando a interoperabilidade das plataformas e aplicações. [4]

2.3.5 PO4 - Definir os Processos de TIC, a Organização e os Relacionamentos

Este processo requer um *framework* de processos de TIC que garanta transparência e controle à organização. Além disso, deve ser estabelecido um comitê estratégico a fim de se criar um Conselho Supervisor de TIC, juntamente com um ou mais comitês direcionadores onde se determine a priorização dos recursos de acordo com as necessidades, bem como os relacionamentos entre a TIC e os negócios. [4]

2.3.6 PO5 - Gerenciar o Investimento

Um *framework* é estabelecido e mantido para gerenciar programas de investimento de TIC. Os *stakeholders* são consultados para identificar e controlar os custos totais e os benefícios no contexto dos planos estratégicos, e também para iniciar ações corretivas onde for necessário. [4]

2.3.7 PO6 - Comunicar o Objetivo e a Direção do Gerenciamento

Este processo visa o desenvolvimento de um sistema de comunicação dentro da organização, a fim de disseminar a missão, os objetivos, as políticas e os procedimentos aprovados e suportados pelo gerenciamento. Esta comunicação é importante para que se alcance os objetivos do setor, uma vez que ela certifica que a organização compreenda os riscos do negócio e da TIC. Desta forma, obtem-se a garantia de que todos os objetivos serão cumpridos atendendo leis e regulamentos relevantes. [4]

[2]Economia de escala é aquela que organiza o processo produtivo de maneira que se alcance a máxima utilização dos fatores produtivos envolvidos no processo, procurando como resultado baixos custos de produção e o incremento de bens e serviços. [20]

2.3.8 PO7 - Gerenciar Recursos Humanos de TIC

Dada a importância das pessoas como recursos estratégicos, bem como a dependência da governança em relação a motivação e competência delas, este processo visa gerenciar os recursos humanos a fim de garantir recrutamento, treinamento, avaliação de performance e promoção ao pessoal de TIC. [4]

2.3.9 PO8 - Gerenciar a Qualidade

Este processo deve manter foco no cliente através de um sistema de gerenciamendo da qualidade, que deve fornecer requerimentos de qualidade claros e bem definidos. Esses requerimentos, por sua vez, devem ser declarados em indicadores quantificáveis e obtíveis. Por fim, deve ser obtida a melhoria contínua através de procedimentos como o monitoramento gradual, a análise e ação sobre desvios, e principalmente na comunicação de resultados aos *stakeholders*, com o objetivo de garantir que o setor está agregando valor ao negócio. [4]

2.3.10 PO9 - Avaliar e Gerenciar os Riscos de TIC

Este processo foca na criação de um framework para avaliação e gerência de riscos, a fim de identificiar e avaliar qualquer possibilidade de impacto nos objetivos da organização, para finalmente, adotar estratégias de contabilização a fim de minimizar os riscos residuais a um nível aceitável. Finalmente, os resultados dessas atividades devem ser disponibilizados em termos financeiros aos *stakeholders*, mantendo o requisito básico de linguagem comum estabelecido pelo COBIT®. [4]

2.3.11 PO10 - Gerenciar Projetos

O PO10 estabelece um *framework* para o gerenciamento de todos os projetos e programas de TIC. O *framework* certifica a correta priorização e coordenação de todos os projetos. Ele tambem inclui um plano mestre, atribuição de recursos, definição de prestações, aprovação de usuários, uma abordagem gradual para a entrega, um plano formal de teste, e a revisão de pós-implementação depois da instalação para certificar o gerenciamento de riscos do projeto e a entrega de valor ao negócio. [4]

2.4 Aquisição e Implementação

O setor de TIC deve gerar soluções adquiridas ou implementadas de forma interativa com os processos de negócio. Isso envolve também as mudanças dos sistemas a fim de garantir que

estes operem com o menor número possível de interrupções. Os processos deste domínio vão cuidar da aquisição e implementação de soluções dentro da organização, fazendo com que o setor seja capaz de discerni-las completamente em qualquer situação, para finalmente, poder decidir concerteza qual é mais interessante em cada momento. [3]

2.4.1 Objetivos de Controle

1. **Métodos de Projeto**

   A metodologia do ciclo de vida de desenvolvimento da organização deve garantir que procedimentos e técnicas apropriados sejam aplicados, a fim de criar as especificações para cada novo projeto de desenvolvimento de sistema, e verificar se essas especificações estão de acordo com os requerimentos do usuário. [2]

2. **Maiores Mudanças nos Sistemas Existentes**

   O gerenciamento deve garantir que no caso de maiores mudanças nos sistemas existentes, um processo de desenvolvimento similar seja observado, como no caso de desenvolvimento de novos sistemas. [2]

3. **Aprovação de Projetos**

   Os responsáveis pelo ciclo de vida devem requerer que as especificações de projeto para todo tipo de desenvolvimento ou modificação de *software* sejam revisadas e aprovadas pelo gerenciamento, usuários afetados e executivos, quando necessário. [2]

4. **Definição de Requerimentos de Arquivo e Documentação**

   A equipe deve garantir que um procedimento apropriado seja aplicado para definir e documentar o formato de arquivo para cada projeto de desenvolvimento ou modificação de sistema. Tal procedimento deve garantir que as regras do dicionário de dados sejam respeitadas[3]. [2]

5. **Especificações de Programa**

   A metodologia do ciclo de vida de desenvolvimento da organização deve requerer que especificações de programas escritas detalhadamente sejam preparadas para cada projeto de desenvolvimento ou modificação de sistema. A metodologia deve, além disso, certificar que as especificações do programa concordam com as especificações do desenho do sistema. [2]

6. **Fonte de Coleta de Dados de Projeto**

[3] O dicionário de dados pode ser definido como um conjunto de todos os elementos de dados pertinentes a um sistema.

É necessário requerer que mecanismos adequados para a coleção e obtenção de dados sejam especificados para cada projeto. [2]

7. **Definição de Requerimentos de Entrada e Documentação**

   Os responsáveis pelo setor devem requerer que mecanismos adequados existam, para definir e documentar os requerimentos de obtenção de dados para cada projeto. [2]

8. **Definição de Interfaces**

   A gerência deve certificar-se que todas as interfaces sejam apropriadamente especificadas, projetadas e documentadas. [2]

9. **Interface Usuário-Máquina**

   Todo projeto deve realizar o desenvolvimento de uma interface entre o usuário e a máquina que seja auto-documentada e fácil de usar. [2]

10. **Definição dos Requisitos de Processamento e Documentação**

    Os responsáveis pela equipe de desenvolvimento devem requerer que mecanismos adequados existam para definir e documentar os requisitos de processamento para cada projeto. [2]

11. **Definição dos Requisitos de Saída e Documentação**

    Os responsáveis pela equipe de desenvolvimento devem requerer que mecanismos adequados existam para definir e documentar os requerimentos de saída para cada projeto. [2]

12. **Controlabilidade**

    O ciclo de vida de desenvolvimento de sistemas da organização deve requerer mecanismos adequados para assegurar que o controle interno, e os requerimentos de segurança sejam especificados para cada projeto de desenvolvimento ou modificação de sistema de informação. Além disso, a metodologia deve garantir que os sistemas de informação sejam projetados de uma forma que garanta a precisão e autorização de entradas, processamento e saídas, dentre outros. Uma avaliação da sensibilidade deve ser realizada no início do desenvolvimento ou modificação do sistema. Os aspectos básicos de segurança e controle interno de um sistema a ser desenvolvido ou modificado devem ser avaliados em sincronia com o projeto conceitual deste, a fim de integrar conceitos de segurança no projeto, tão cedo quanto for possível. [2]

13. **Disponibilidade como Fator Chave de Projeto**

    Os responsáveis pelo desenvolvimento devem garantir que a disponibilidade seja considerada nos projetos de sistemas o quanto antes for possível. A disponibilidade deve

ser analisada e, se necessário, aumentada através de melhorias na manutenção e na segurança. [2]

14. **Provisões de Integridade de TIC em *Softwares* Aplicativos**

    A organização deve estabelecer procedimentos que certifiquem, onde for aplicável, que os aplicativos contenham provisões que rotineiramente verifiquem as tarefas realizadas pelo *software* para ajudar a certificar a integridade dos dados, e fornecer a restauração da integridade através da reversão ou outros meios. [2]

15. **Teste de *Softwares* Aplicativos**

    Testes unitários, testes de aplicação, testes de integração, testes de sistema e testes de carga e estesse devem ser realizados de acordo com o plano de testes bem como os padrões de teste estabelecidos, antes da aplicação ser aceita pelo usuário. Medidas adequadas devem ser conduzidas a fim de prevenir a divulgação de informações importantes utilizadas durante o teste. [2]

16. **Referência de Usuários e Materiais de Suporte**

    A organização deve garantir que referências de usuário adequadas e manuais de suporte sejam preparados como parte de todo projeto de desenvolvimento ou modificação de sistema. [2]

17. **Reavaliação de Projeto de Sistema**

    A organização deve garantir que o projeto do sistema seja reavaliado sempre que significantes discrepâncias técnicas ou lógicas ocorram durante o seu desenvolvimento ou manutenção. [2]

2.4.2 AI1 - Identificar Soluções Automatizadas

Este processo é responsável por avaliar se as necessidades apresentadas no ambiente de TIC, sejam elas de novas aplicações ou funções, atendem aos requisitos de negócio de forma eficiente. Além disso, devem ser feitas análises de risco e de custo-benefício, para finalmente, decidir se é viável produzir ou comprar a solução necessária. Se for selecionada a compra, devem ser feitas considerações sobre fontes alternativas, levando em consideração a performance e a efetividade de custo dessas fontes, além de outros fatores relevantes à organização. Tudo isso a fim de reduzir os custos para adquirir e implementar soluções, de uma forma que não coloque em risco os objetivos do negócio. [4]

2.4.3 AI2 - Adquirir e Manter o *Software* Aplicativo

Este processo é responsável por manter o projeto e os requisitos de segurança das aplicações de acordo com os padrões estabelecidos. Essas aplicações devem ser disponibilizadas em sincronia com os requisitos de negócio, a fim de permitir que a organização suporte suas operações de negócio com soluções corretas. [4]

2.4.4 AI3 - Adquirir e Manter a Infra-estrutura Tecnológica

Este processo define procedimentos direcionados a manter a infra-estrutura tecnológica de acordo com as estratégias acordadas, adquirindo, implementando e atualizando tudo o que for relacionado a ela, a fim de garantir a existência de um sólido suporte tecnológico para as aplicações e processos de negócio. [4]

2.4.5 AI4 - Habilitar a Operação e o Uso

Este processo visa garantir que todos os novos sistemas sejam utilizados da melhor forma possível, fazendo com que os usuários conheçam todos os recusos disponibilizados. Para isso, devem ser realizados treinamentos, bem como desenvolvidas a documentação e os manuais de cada sistema. [4]

2.4.6 AI5 - Adquirir Recursos de TIC

Este processo deve garantir que todos os recursos de TIC necessários para atender as necessidades do negócio estejam disponíveis a tempo, e principalmente com custos reduzidos. Esses recursos incluem pessoas, *hardware*, *software* e serviços, que devem ser adquiridos através de procedimentos pré-definidos, selecionando vendedores e elaborando a configuração dos regimes contratuais. [4]

2.4.7 AI6 - Gerenciar Mudanças

Este processo deve garantir uma gerência de mudanças efetiva, a fim de assegurar que todos os riscos que possam impactar negativamente no ambiente de produção sejam mitigados e resolvidos. Isso é possível quando se possui controle sobre todos os tipos de mudanças realizadas no ambiente, fazendo com que elas sejam registradas, avaliadas e autorizadas antes da sua realização. Além disso, é necessária uma revisão com relação aos resultados planejados, logo após a implementação dessas mudanças. [4]

2.4.8 AI7 - Instalar e Credenciar Soluções e Mudanças

Este processo deve testar os novos sistemas antes de promovê-los ao ambiente de produção, a fim de garantir que eles estejam de acordo com as expectativas e os resultados acordados. Esses testes devem ser feitos em ambientes dedicados e com dados relevantes, aplicando instruções de mitigação. Por fim, deve ser desenvolvida uma revisão de pós implementação. [4]

2.5 Entrega e Suporte

Este domínio está preocupado com a entrega dos serviços solicitados, que inclui o gerenciamento da segurança e continuidade, suporte de serviço para os usuários, e o gerenciamento de dados e de facilidades operacionais. Ele tipicamente trata de questões como, por exemplo, o alinhamento da entrega de serviços com as prioridades do negócio, a otimização dos custos de TIC, o uso produtivo e seguro dos sistemas de TIC e a segurança da informação. [3]

2.5.1 Objetivos de Controle (*Control Objectives*)

Garantir a Segurança dos Sistemas

1. **Gerenciar Medidas de Segurança**

   A segurança de TIC deve ser gerenciada de forma que as medidas de segurança estejam de acordo com os requerimentos de negócio, e isso inclui: [2]

   - Traduzir as informações da avaliação de riscos aos planos de segurança de TIC;
   - Implementar o plano de segurança de TIC;
   - Atualizar o plano de segurança de TIC com o objetivo de refletir as mudanças na configuração do setor;
   - Avaliar o impacto das requisições de mudança na segurança de TIC;
   - Monitorar a implementação do plano de segurança de TIC;
   - Alinhar os procedimentos de segurança de TIC com outras políticas e procedimentos.

2. **Identificação, Autenticação e Acesso**

   O acesso lógico e o uso dos recursos computacionais de TIC devem ser restringidos pela implementação de mecanismos de identificação, autenticação e autorização adequados, fazendo o *link* entre usuários e recursos através de regras de acesso. Tais mecanismos devem proibir pessoal não-autorizado, minimizar a necessidade de usuários autorizados

utilizarem múltiplos *logins*. Além disso, devem haver procedimentos que mantenham a efetividade dos mecanismos de autenticação e acesso (ex: trocas periódicas de senhas). [2]

3. **Segurança no Acesso *Online* de Dados**

   Em um ambiente *online*, o gerenciamento de TIC deve implementar procedimentos em sinergia com as políticas de segurança que forneçam controle de segurança de acesso baseada nas necessidades individuais demonstradas de visualizar, adcionar, alterar ou deletar dados. [2]

4. **Gerenciamento de Contas de Usuário**

   O gerenciamento deve estabelecer procedimentos para garantir ações realizadas a tempo de requisitar, estabelecer, caracterizar, suspender e encerrar contas de usuário. Um procedimento de aprovação formal delineando os dados e garantindo os privilégios de acesso deve ser incluído. A segurança de acesso de terceiros deve ser definida contratualmente e endereçar requerimentos não divulgados. Regimes de subcontratação devem endereçar os riscos, controles de segurança e procedimentos para sistemas de informação no contrato entre as partes. [2]

5. **Revisão de Gerenciamento de Contas de Usuário**

   É necessário que o gerenciamento possua um processo de controle com o objetivo de rever e confirmar os direitos de acesso periodicamente. A comparação periódica de recursos com responsabilizações registradas deve ser realizada a fim e ajudar a reduzir o risco de erros, fraude, uso incorreto ou alteração não autorizada. [2]

6. **Controle do Usuário sobre as Contas**

   Os usuários devem poder controlar as atividades de suas próprias contas. Mecanismos informativos devem estar à disposição a fim de permiti-los a vigiar as atividades normais, bem como de ser alertado sobre atividades incomuns em um curto espaço de tempo. [2]

7. **Fiscalização de Segurança**

   A administração da segurança de TIC deve certificar que suas atividades sejam devidamente registradas, e qualquer indicação de violação de segurança iminente deve ser reportada imediatamente a todos os interessados (interna e exernamente) e atendidas a tempo. [2]

8. **Classificação de Dados**

   O gerenciamento deve implementar procedimentos que garantam a classificação de todos os dados em termos de sensibilidade, por uma decisão formal e explícita do dono da informação, de acordo com o esquema de classificação de dados. Mesmo os dados

que não necessitem de proteção devem requerer uma decisão formal para que sejam diferenciados. Os donos devem determinar a disposição e o compartilhamento dos dados, bem como se e quando os programas e arquivos devem ser mantidos, arquivados ou deletados. A aprovação dos donos e a disposição dos dados deve ser mantida. Políticas devem ser definidas a fim de suportar a reclassificação da informação, baseada nas sensibizações de mudanças. O esquema de classificação deve incluir critérios para gerenciar trocas de informação entre organizações, endereçando a segurança à legislação relevante. [2]

9. **Identificação Central e Gerenciamento de Direitos de Acesso**

   Os controles estão em posição de certificar que a identificação e os direitos de acesso dos usuários bem como a identidade do sistema sejam estabelecidos e gerenciados de uma maneira única e central, a fim e obter consistência e eficiência no controle de acesso global. [2]

10. **Relatórios de Violação e de Atividades de Segurança**

    A administração de segurança de TIC deve garantir que as violações e as atividades de segurança sejam registradas, reportadas, revisadas e apropriadamente escaladas em uma base regular a fim e identificar e resolver incidentes envolvendo atividades não autorizadas. As informações responsáveis pelo acesso lógico aos recursos computacionais devem ser baseadas na hierarquia de privilégio ou de necessidade de conhecimento. [2]

11. **Tratamento de Incidentes**

    O gerenciamento deve estabelecer um mecanismo de tratamento de incidentes, capaz de endereçar os incidentes de segurança, e fornecendo assim uma plataforma com perícia e equipada com facilidades de comunicação rápidas e seguras. Os procedimentos e as responsabilidades do gerenciamento de incidentes deve ser estabelecido para certificar uma resposta apropriada, efetiva e rápida aos incidentes de segurança. [2]

12. **Recredenciamento**

    É necessário que o gerenciamento garanta o recredenciamento periódico da segurança, a fim de atualizar o nível de segurança formalmente aprovado e a aceitação do risco residual. [2]

13. **Confiança da Contraparte**

    A política organizacional deve garantir que práticas de controle sejam implementadas a fim de verificar a autenticidade da contraparte fornecendo instruções eletrônicas ou transações. Isto pode ser implementado através de trocas senha confiáveis, símbolos ou chaves criptografadas. [2]

14. **Autorização de Transações**

    É extremamente necessário que a política organizacional certifique que, onde necessário, sejam implementados controles a fim de prover autenticidade de transações e estabelecer a validade de uma identidade reivindicada ao sistema. Isto requer o uso de técnicas de criptografia para acessar e verificar transações. [2]

15. **Não-repúdio**

    A política organizacional deve garantir que as transações não possam ser danificadas por qualquer parte, e que sejam implementados controles para prover a não-repudiação de origem ou destino, provando a submissão e a recepção das transações. Isso pode ser implementado através de assinaturas digitais e *timestamping*[4], dentre outros, com políticas apropriadas que levem em consideração relevantes requisitos regulatórios. [2]

16. **Caminho Confiável**

    Uma garantia de que os dados transacionais sejam trocados apenas sob um caminho confiável deve ser oferecida pela poítica organizacional. O conjunto de informações sensíveis inclui desde dados do gerenciamento da segurança até chaves criptografadas. Para alcançar este objetivo, canais de comunicação confiáveis devem ser estabelecidos, utilizando criptografia entre usuários, entre usuários e sistemas, e finalmente, entre sistemas. [2]

17. **Proteção de Funções de Segurança**

    Todo *software* e *hardware* relacionado à segurança deve ser protegido a todo tempo contra adulteração e divulgação de chaves secretas a fim e manter sua integridade. Ademais, as organizações devem ser discretos com relação ao seu projeto de segurança, mas não devem embasar sua segurança em manter esse projeto secreto. [2]

18. **Gerenciamento de Chaves Criptografadas**

    O gerenciamento deve definir e implementar protocolos e procedimentos capazes de garantir a proteção de chaves contra qualquer modificação não-autorizada. Se uma chave é comprometida, o gerenciamento deve certificar-se de que essa informação seja disseminada a toda e qualquer parte interessada, através de listas de anulação de certificado ou mecanismos similares. [2]

19. **Prevenção, Detecção e Correção de *Software* Malicioso**

    Com relação aos *softwares* maliciosos tais como vírus e *trojans*, o gerenciamento deve estabelecer um *framework* de medidas de controle preventivas, detectivas e corretivas,

[4] *Timestamping* ou *Trusted Timestamping* é uma técnica utilizada em sistemas de informação para registrar de forma confiável (que ninguém possa alterar) os momentos de criação e modificação de um dado documento. [16]

com efetividade de resposta a ocorrências e relatórios. O negócio e o gerenciamento de TIC devem garantir que esses procedimentos sejam estabelecidos através da organização, a fim de proteger seus sistemas de informação deste tipo de problema. [2]

20. **Arquiteturas de *Firewall* e Conexões com Redes Públicas**

    Se a conexão com a internet ou qualquer outra rede pública existir, firewalls adequados devem ser operados a fim de oferecer proteção contra ataques *Denial of Service* (DOS) acesso não autorizado a recursos internos, e além disso, controlar todo o fluxo de gerenciamento de aplicação ou infra-estrutura, em ambas as direções. [2]

21. **Proteção do Valor Eletrônico**

    O gerenciamento deve primar pela integridade continuada de todos os cartões ou mecanismos físicos similares utilizados para autenticação ou armazenamento de informações valiosas, levando em consideração as facilidades relacionadas, os dispositivos, os empregados e os métodos de validação utilizados. [2]

2.5.2 DS1 - Definir e Gerenciar Níveis de Serviço

Este processo deve definir e gerenciar os níveis de serviço, a fim de garantir que todas as metas e requistos de serviços estabelecidos nos acordos entre a organização e o cliente sejam cumpridos. Para isso, devem ser elaborados acordos intra-organizacionais e contratos, objetivando garantir a qualidade das soluções de suporte aos serviços prestados pelo setor de TIC, de forma que os acordos aplicam-se às outras áreas de negócio dentro da organização, e os contratos aos fornecedores externos. [4]

2.5.3 DS2 - Gerenciar Serviços de Terceiros

Este processo, através da definição de papéis, responsabilidades e expectativas nos contratos, deve garantir que todos os serviços terceirizados estejam de acordo com os requisitos do negócio. Além disso, é necessário que esses serviços sejam monitorados, buscando sempre a garantia de que os serviços prestados não serão prejudicados por requisitos dependentes de fontes externas. Com isso, é possível minimizar os riscos de negócio associados a fornecedores improdutivos. [4]

2.5.4 DS3 - Gerenciar a Performance e a Capacidade

Este processo objetiva garantir que a o setor de TIC tenha capacidade de suportar os futuros objetivos do negócio, garantindo performance e disponibilidade aos serviços. Para

isso, são necessárias previsões de necessidades baseadas em carga de trabalho, armazenamento e requisitos de contingência. Por fim, vale ressaltar que o sucesso destes objetivos depende diretamente da qualidade da gerência de demanda. [4]

2.5.5 DS4 - Garantir a Continuidade dos Serviços

Este processo deve garantir que os serviços de TIC nos principais processos e funções de negócio tenham a mínima probabilidade possível de sofrer uma interrupção, e na iminência desta, que eles sejam suficientemente resilientes, a fim de garantir a continuidade do negócio. Isso é alcançável através da aplicação de técnicas como o *offsite backup*[5], e principalmente, fornecendo um treinamento periódico relativo ao plano de continuidade da organização. [4]

2.5.6 DS5 - Garantir a Segurança dos Sistemas

Este processo deve proteger todos os ativos de TIC, objetivando a minimização de impactos no negócio causados por possíveis incidentes ou vulnerabilidades de segurança. Para isso, devem ser realizados monitoramentos, testes e correções de problemas periodicamente, eliminando assim todas as fraquezas ou incidentes de segurança. [4]

2.5.7 DS6 - Identificar e Alocar Custos

Este processo deve desenvolver um sistema com a função de capturar, armazenar e reportar os custos de TIC aos usuários, a fim de ajudar os executivos a tomar decisões mais precisas sobre o uso dos serviços. Para isso é necessária uma avaliação precisa e uma modelagem dos custos de TIC, além de um acordo que busque uma alocação de custos mais razoável com os usuários do negócio. [4]

2.5.8 DS7 - Educar e Treinar Usuários

Este processo visa aumentar o uso efetivo das tecnologias, bem como dos recursos inerentes a elas, a fim de diminuir o número de erros de usuários, aumentar a produtividade e o cumprimento de medidas de segurança. Para isso, é necessário que as necessidades de treinamento de cada grupo sejam identificadas, para que finalmente, seja desenvolvido um programa de treinamento efetivo. [4]

[5] O *offsite backup* ou *vaulting* é a estratégia de armazenar dados críticos para fora de sua localização principal. Esta estratégia é muito utilizada por exemplo nos Planos de Continuidade de Negócio.

2.5.9 DS8 - Gerenciar a Central de Serviços e os Incidentes

Este processo deve cuidar para que todos os incidentes sejam resolvidos com o menor tempo possível, aumentando assim a sustentabilidade das soluções ofertadas pela organização. Tal objetivo pode ser alcançado através de uma Central de Serviços bem elaborada, com credibilidade suficiente para que todos os clientes solicitem manutenções através dela. Um processo de Gerenciamento de Incidentes bem estruturado, por fim, fará com que todos os incidentes de solução conhecida sejam atendidos com o menor tempo possível. Essas atividades aumentam a produtividade dos usuários, além de gerar conhecimento para posteriores descobertas de causas raíz (problemas). [4]

2.5.10 DS9 - Gerenciar a Configuração

Este processo deve garantir a integridade das configurações de *hardware* e *software* da organização. Para isso são necessárias atividades como o estabelecimento de *baselines*, a verificação das informações de configuração e a atualização do repositório de configuração, conforme for necessário. Tudo isso a fim de aumentar a disponibilidade dos sistemas, e eliminar restrições relativas a produtividade de usuários. [4]

2.5.11 DS10 - Gerenciar Problemas

Este processo deve cuidar para que todas as causas raíz de incidentes sejam identificadas e eliminadas (através de mudanças), a fim de reduzir custos, maximizar a disponibilidade do sistema e melhorar os níveis de serviço, o que contribui diretamente para a melhoria do conforto e da satisfação do cliente. [4]

2.5.12 DS11 - Gerenciar Dados

Este processo deve gerenciar a biblioteca de mídia, o *backup* e a recuperação de dados, identificando os seus requisitos e definindo procedimentos para atendê-los, a fim de ajudar a garantir a qualidade e a disponibilidade de dados em tempo útil. [4]

2.5.13 DS12 - Gerenciar o Ambiente Físico

Este processo tem como principal objetivo reduzir as interrupções de negócio ocasionadas por danos em computadores ou pessoas, aumentando assim a produtividade do setor. Isso é possível quando o ambiente dispõe de facilidades físicas, com requisitos bem definidos e atendidos, e finalmente, quando se gerencia o acesso físico ao local. [4]

2.5.14 DS13 - Gerenciar Operações

Este processo deve definir políticas de operação, monitorar a performance da infra-estrutura e realizar manutenções preventivas de *hardware*, a fim de manter a integridade dos dados, reduzindo assim os atrazos de negócio e os custos das operações de TIC. [4]

2.6 Monitoramento e Avaliação

Todo processo de TIC deve ser regularmente avaliado para que sua qualidade e o cumprimento dos requisitos de controle sejam válidos no decorrer do tempo. Este domínio abre as portas do setor para o gerenciamento de performance, monitoramento de controle interno, cumprimento regular de requisitos e, finalmente, a governança. Tipicamente, são avaliadas questões como a deteção de problemas em tempo hábil através de medidas de performance, a garantia da eficiência e efetividade do controle interno e o alinhamento com os objetivos do negócio. [3]

2.6.1 Objetivos de Controle

1. **Coletar Dados de Monitoramento**

   Para a TIC e o processo de controle interno, o gerenciamento deve garantir que os KPIs relevantes de fontes internas ou externas sejam bem definidos, e que os dados por eles fornecidos sejam coletados para que se possa criar os relatórios relativos à essas informações. Os controles devem focar-se em validar a integridade desses KPIs. [2]

2. **Avaliar a Performance**

   Os serviços a ser entregues pelas funções de TIC devem ser medidos (KPIs ou CSFs) pelo gerenciamento e comparados com os níveis almejados. Avaliações das funções de TIC devem ser realizadas em uma base contínua. [2]

3. **Avaliar a Satisfação do Cliente**

   Em intervalos regulares, o gerenciamento deve medir a satisfação do cliente com relação aos serviços entregues pelas funções de TIC, a fim de identificar deficiências nos níveis de serviço, e assim estabelecer objetivos de melhoria. [2]

4. **Relatórios de Gerenciamento**

   Relatórios de gerenciamento devem ser fornecidos para que os executivos possam revisar e avaliar o progresso da organização com relação aos objetivos relacionados. Esses relatórios devem incluir as extensões que os objetivos planejados devem alcançar, os

resultados obtidos, as metas de performance alcançadas e os riscos mitigados. Após a revisão, ações apropriadas de gerenciamento devem ser iniciadas e controladas. [2]

2.6.2 ME1 - Monitorar e Avaliar a Performance de TIC

Este processo deve monitorar o ambiente a fim de garantir a integridade do trabalho realizado, para que este esteja de acordo com o conjunto de direções e políticas da organização. Os monitoramentos devem ser realizados através de KPIs relevantes, relatórios de performance sistemáticos e da atuação direta sobre os desvios identificados. [4]

2.6.3 ME2 - Monitorar e Avaliar o Controle Interno

Este processo deve definir um programa de controle interno para o setor de TIC, a fim de garantir operações efetivas e eficientes, bem como o cumprimento de todas as regulamentações aplicáveis. O programa, por sua vez, requer um processo de monitoramento que inclui os resultados da exceções de controle, das auto-avaliações e das revisões de terceiros. [4]

2.6.4 ME3 - Assegurar a Conformidade com Requisitos Externos

Este processo visa estabelecer um procedimento de revisão a fim de garantir que os requisitos de conformidade estejam de acordo com os requisitos contratuais. Isso envolve ações como identificar os requisitos de conformidade e avaliar os responsáveis, para que finalmente possa ser realizada uma integração entre os relatórios de conformidade do setor de TIC com o negócio. [4]

2.6.5 ME4 - Prover Governança de TIC

Estabelecer um framework de governança efetivo requer a definição de estruturas organizacionais, processos, liderança, papéis e responsabilidades para que se possa garantir que os investimentos no setor de TIC estejam sendo utilizados de maneira ótima, com custos reduzidos e, principalmente, de acordo com as estratégias do negócio. [4]

3 *ITIL® V3*

A Biblioteca ITIL® V3 foi criada na década de oitenta pelo governo britânico a partir de práticas utilizadas por empresas de sucesso na época, com o objetivo de se criar um padrão para o gerenciamento de serviços de TIC. Essa biblioteca cresceu muito ao longo dos anos, e nos dias de hoje se tornou o framework mais aceito para o gerenciamento de serviços de TIC no mundo.

Para falar sobre este framework, são necessários alguns conceitos apresentados a seguir:

3.1 Definição de Serviço:

"Um serviço é uma maneira de entregar valor ao cliente facilitando os resultados que ele quer atinjir sem a posse dos custos e riscos específicos." [13]

Os resultados, por sua vez, são possíveis a partir do desepenho de tarefas, e limitados por algumas restrições. Resumidamente, os serviços facilitam os resultados reforçando a performance dessas tarefas e reduzindo o conjunto de restrições. Alguns serviços podem ser a própria realização de uma tarefa.

3.2 Composição do Valor do Serviço:

Partindo da perspectiva do cliente, o valor de um serviço é composto por sua utilidade ou aptidão para o propósito (fitness for purpose) e garantia, ou aptidão para o uso (fitness for use).

A utilidade do serviço é comprovada quando este provoca melhorias na performance de alguma tarefa, ou ainda quando se reduz o conjunto de restrições para que essas tarefas tenham uma performance ótima.

A garantia do serviço é comprovada a partir da continuidade e segurança que ele apresenta.

Características e desafios que distinguem os serviços de outros sistemas de criação de valor (Ex: Agricultura) [13]

- Natureza intangível da saída (retorno) do serviço - É dificil medir o valor que ele possui.
- Demanda estreitamente embutida nos ativos do cliente - Usuários, aplicações e documentos geram demanda e estimulam a produção de serviço.
- Alto nível de contato entre produtores e consumidores de serviço.
- Natureza perecível da saída (retorno) e da capacidade do serviço. Existe a necessidade de manter o cliente com a certeza de que o serviço vai continuar a ser prestado com qualidade consistente.

Os modelos de negócio inovadores juntamente com as inovações tecnológicas vêm contribuindo ao longo dos anos com o desafio de tornar estas restrições mais amenas, logo, pode-se dizer que atualmente essas restrições não são características universais.

3.3 O Ciclo de Vida do ITIL®

Atualmente na versão 3, a ITIL® trabalha encima de um ciclo de vida de 5 (cinco) etapas, onde cada uma contém um livro que descreve seus processos, funções, papéis e recursos necessários. São eles:

3.3.1 Estratégia de Serviço

É a parte do ciclo de vida onde o setor de TIC vai se integrar com o setor de negócios, com o objetivo de evitar a falta de recursos e de tempo para a realização de suas atividades do cotidiano. Isso é possível quando se tem conhecimento da demanda dos clientes, do *pipelining* de serviços do catálogo e também dos recursos disponíveis ao setor de TIC. [13]

3.3.2 Desenho de Serviço

É a fase do ciclo de vida onde o serviço será projetado de acordo com os dados levantados na fase estratégica, considerando a demanda dos clientes desse serviço, a elaboração dos acordos de nível de serviço, acordo de nível operacional e contratos. Além disso, nesta etapa são feitas outras inúmeras considerações que serão detalhadas no final deste trabalho. [15]

3.3.3 Transição de Serviço

Tendo o serviço já desenvolvido, a etapa de transição de serviço cuida da tarefa de colocá-lo em produção, sem afetar os demais serviços existentes já em funcionameto. Esta etapa

considera que para colocar um serviço em produção, pode ser necessária uma mudança na estrutura atual do setor de TIC. Por sua vez, essas mudanças devem ser totalmente planejadas, já que elas são uma das maiores causas de *downtimes* em setores de TIC na maioria dos casos registrados por empresas do mundo todo. [14]

3.3.4 Operação de Serviço

Esta fase pode ser considerada o cotidiano da organização. É onde ocorrem os incidentes, problemas, solicitações de serviço, retiradas de serviço, etc. Nesta fase a organização tem a responsabilidade de coordenar e conduzir as atividades e processos requeridos, para entregar e gerenciar serviços nos níveis acordados com usuários e clientes do negócio. [11]

3.3.5 Melhoria de Serviço Continuada

Esta fase é uma das mais importantes do ciclo, onde os gerentes devem estabelecer um círculo contínuo de monitoração e *feedback*, encontrando oportunidades de melhoria dentro de todas as outras fases do ciclo de vida do serviço. Entre os principais resultados obtidos aqui está o aumento do aprendizado/conhecimento dos gerentes em relação aos serviços, permitindo um maior alinhamento do setor de TIC às necessidades do negócio, no que tange a qualidade, custos e prazos. [12]

O Gerenciamento de Serviços se interresa em mais do que apenas entregar serviços. Ele assume um conjunto de práticas que envolvem o serviço desde o nascimento da necessidade até a sua entrega como solução, envolvendo etapas importantes para o valor do serviço, como por exemplo, a elaboração de contratos (com terceiros) que irão influenciar na qualidade do serviço prestado. [17]

As entradas (*Inputs*) para o gerenciamento de serviços são os recursos e as capacidades que representam as características do provedor de serviço. As saídas são os serviços, que por sua vez, entregam valor aos clientes ou usuários.

O gerenciamento de serviço efetivo é uma característica estratégica do provedor de serviço, e lhe fornece a habilidade de lidar com o núcleo do negócio, fazendo com que ele entregue serviços que agreguem valor ao cliente, tornando mais fácil o caminho para que este atinja com facilidade os objetivos almejados.

3.4 Processos

"Um processo é um conjunto de atividades cordenadas combinando e implementando recursos e capacidades com o objetivo de produzir um resultado, que direta ou indiretamente, cria valor para um cliente externo ou stakeholder." [13]

Processos da Fase Estratégia de Serviço

3.4.1 Gerenciamento do Portfolio de Serviço

O objetivo do processo de Gerenciamento de Portifolio de Serviço é estabelecer uma base de decisão no direcionamento de estratégias e gerenciamento de investimentos em serviço. É deste processo a responsabilidade de cuidar do pipeline de serviços, do catálogo de serviços e também da lista de serviços retirados. [13]

O portifolio de serviços possui todos os serviços que estão sendo prestados, independente de sua localização no ciclo de vida.

Fazem parte do pipeline de serviços os serviços que estão em vista da empresa (espaços de mercado), os que estão sendo projetados, em transição ou até na fase de melhoria.

Fazem parte do catálogo de serviços os serviços que estão em transição, operação ou sendo retirados.

3.4.2 Gerenciamento da Demanda

O objetivo do processo de Gerenciamento da Demanda é entender os padrões de atividade do Negócio e influenciar a demanda do Cliente por serviços e a provisão de capacidade para atender estas demandas. [13]

O aumento da demanda nos processos de negócio, aumenta de forma não linear as necessidades dos serviços de TIC e os 4 P's[1].

Uma das contribuições mais importantes do Gerenciamento da Demanda é na elaboração do plano de capacidade da organização. O plano de capacidade tem como principal objetivo a prevenção de problemas futuros na organização.

Não conhecer a demanda de um cliente implica diretamente em desperdiçar recursos se a capacidade estimada for além da necessária, ou ainda, na impossibilidade de atender o negócio, se a capacidade estimada for menor que a necessária. Ambos vão resultar no desperdício de

[1]Os 4 P's são: Pessoas, Processos, Produtos (tecnologias, ferramentas e serviços) e Parceiros (fabricantes, fornecedores)

dinheiro.

É muito importante também que o setor de TIC seja capaz de influenciar a demanda dos outros setores. Isso pode ser possível através da contabilização do uso de recursos entre outros setores. Essa contabilização pode, por exemplo, ajudar a diferenciar e a descobrir as áreas de negócio mais eficientes.

3.4.3 Gerenciamento Financeiro

O objetivo do processo de Gerenciamento Financeiro é prover ao negócio e à TIC a quantificação, em termos financeiros, do valor dos Serviços de TIC, do valor dos ativos que sustentam o provisionamento destes serviços e a qualificação da previsão operacional financeira (orçamento). [13] Dentre os principais conceitos dentro deste processo, destacam-se:

- **Análise de Investimento:** Tem a função de produzir valor ao longo do ciclo de vida do serviço, a partir do valor recebido e dos custos incorridos. Isto proverá modelos analíticos e conhecimento para levantar o valor esperado e/ou o retorno de uma determinada iniciativa, solução, programa ou projeto de uma maneira padronizada.
- **Contabilização:** É o sub-processo responsável por identificar custos atuais da entrega de serviços de TIC, comparando-os com os custos previstos e gerenciando a variação do orçamento. Isto vai alterar a dinâmica e visibilidade do Gerenciamento de Serviço, permitindo um maior nível de desenvolvimento e execução da Estratégia de Serviço.

  Este sub-processo ainda fará a contabilização dos custos associados a cada serviço. Esses custos podem ser relacionados a:

  - Hardware
  - Software
  - Pessoal
  - Acomodação
  - Transferência

  E finalmente, podem ser classificados como:

  - Custo Operacional e de Capital
  - Custo Direto (tem parcela definida por serviço. Ex: mão-de-obra) e Indireto (depende de um critério de rateio. Ex: Aluguel).
  - Custo fixo e variável
  - Unidades de Custo

- **Cobrança:** As atividades deste processo são divididas entre 3 centros, são eles:
  - Centro de Contabilização, que objetiva simplesmente alocar os custos.
  - Centro de Recuperação, que objetiva alocar e dividir esses custos em partes proporcionais.
  - Centro de Lucro - Objetiva dar autonomia suficiente para operar como uma entidade de negócio separada, mas com os objetivos de negócio estabelecidos pela Organização.
- **Caso de Negócio** *(business case)*: é uma ferramenta de planejamento e suporte à decisão que projeta as prováveis consequências de uma ação de Negócio. O uso dessa ferramenta se mostra extremamente eficiente durante o ciclo de estratégia do serviço.

Processos da Fase Desenho de Serviço

3.4.4 Gerenciamento de Nível de Serviço

O Processo de Gerenciamento de Nível de Serviço (SLM - *Service Level Management*)é a interface entre o setor de TIC e a Área de Negócio, pois converte os requisitos de negócio em Metas de Nível de Serviço que deverão ser atendidas pelo setor. Seu principal objetivo é negociar, definir e documentar os acordos e metas apropriadas para os serviços de TIC juntamente com o representante do Negócio. [15]

Este processo também define maneiras para que seja feito um monitoramento com o objetivo de produzir relatórios relativos a capacidade do provedor de entregar o serviço de TIC no nível acordado. Resumidamente, ele entende a necessidade do negócio e prepara o setor de TIC para fornecer o serviço.

O SLM é um dos principais responsáveis por gerar dados para os sistemas de Gerenciamento da Configuração e do Conhecimento, pois vai coletar direto da fonte os dados relativos aos serviços prestados à outras áreas de negocio (dentro da organização), a outras organizações e também os dados relativos a serviços adquiridos (terceirizados).

Conceitos e Definições:

- **Requisito de Nível de Serviço (SLR - *Service Level Requirement*)**

  Baseados nos objetivos do Negócio, os SLR são utilizados para fazer a negociação das Metas de Nível de Serviço. Resumidamente, um SLR pode ser definido como um requisito do cliente para aspectos relativos a entrega de um Serviço de TIC.

- **Meta de Nível de Serviço (SLT - *Service Level Targets*)**

Uma SLT é um compromisso, baseado nas SLR, que vai ser documentado em um Acordo de Nível de Serviço. Os termos deste acordo serão um conjunto de SLTs, ou seja, é através da medição destas que será possível concluir se um provedor realizou ou nao o serviço que foi contratado, realizando todas as tarefas ou ainda eliminando todas as restrições acordadas. Por este motivo, as SLT devem ser declaradas em formato SMART (*Specific, Measurable, Achiievable, Results Oriented and Time Specifc* - Específico, Mensurável, Realizável, Relevante e em Tempo). Uma forma de se obter este resultado é baseá-las em Indicadores de Desempenho.

- **Definição de Requisitos (SOR - *Statement Of Requirements*)**

  Um documento que descreve todas as funcionalidades e requisitos necessários a um serviço, seja ele novo ou mudado.

- **Acordo de Nível de Serviço (SLA - *Service Level Agreement*)**

  O Acordo de Nível de Serviço visa garantir a disponibilidade do serviço de TIC para o Processo de Negócio (cliente). Nele estão contidas as SLT, que seguindo as SLR, especificam as responsabilidades do Provedor de Serviço de TIC e do Cliente. Um SLA pode ser classificado em três diferentes tipos, a saber:

  - **SLA baseado em Serviço**

    É um SLA escrito para cobrir um tipo específico de serviço, para todos os clientes que contratarem aquele serviço. Por exemplo, um provedor de internet que escreve um SLA para cada plano (serviço) que ele visa fornecer, e todos os clientes que adiquirirem um mesmo plano vão assinar um mesmo SLA.

  - **SLA baseado em Cliente**

    É um SLA escrito especificamente para um determinado cliente, abrangendo todos os serviços que ele adiquirir.

  - **SLA Multi-Nível**

    Exitem organizações que adotam estruturas multi-nivel para SLAs, criando uma hierarquia de acordos. Primeiramente é feito um SLA de nível corporativo, contendo informações necessárias para a elaboração de qualquer acordo a ser utilizado pela organização. Em seguida, é elaborado um SLA a nível de cliente, que vai cobrir todos os assuntos relevantes para um grupo de clientes ou unidades de negócio, independentemente dos serviços.

- **Acordo de Nível Operacional (OLA - *Operational Level Agreement*)**

  Os Acordos de Nível Operacional são utilizados para suportar a entrega de serviços acordados entre áreas de negócio que se encontram dentro da mesma organização. Neste caso, este acordo seria entre o setor de TIC e qualquer outro setor da empresa. O OLA tem

por objetivo definir os produtos e/ou serviços providos e as responsabilidades de ambas as partes.

- **Contrato de Apoio (UC - *Underpinning Contract*)**

  Os Contratos de Apoio são utilizados para definir, de forma legal, as metas e responsabilidades necessárias para se adquirir bens ou serviços de um terceiro, a fim de atender uma ou mais SLTs acordadas em um SLA.

Além desses conceitos, são apresentadas atividades que precisam ser desempenhadas para que o SLM seja realizado com sucesso. Essas atividades são listadas como segue:

- Realizar a determinação, negociação, documentação e acordo dos requisitos para o serviço, seja ele novo ou alterado, nos SLR.
- Gerenciar esses SLR nos SLA, através do Ciclo de Vida do Serviço.
- Monitorar e comparar, através de KPIs, o desempenho do serviço com as SLTs acordadas em todos os SLAs.
- Sempre medir a satisfação do cliente, visando agir para melhorá-la.
- Gerar relatórios dos serviços.
- Revisar os serviços acordados e estimular a melhoria dos mesmos através de um Plano de Melhorias do Serviço (SIP). Um SIP é um conjunto de ações de melhoria priorizadas, que engloba todos os serviços e processos.
- Manter procedimentos eficientes em registrar e solucionar todas as reclamações.

Dos papéis tangíveis a este processo, vale citar o Gerente de Nível de Serviço (*Service Level Manager*), que é o responsável por garantir que os objetivos do SLM sejam atingidos.

Por fim, para a realização deste processo surgem alguns desafios, como por exemplo:

- Realizar a identificação dos representantes legais do cliente, ou seja, com quem devem ser feitos os acordos.
- Melhorar o relacionamento e comunicação com o Negócio e Clientes.
- Garantir metas mensuráveis e específicas para todos os serviços.
- Garantir pró-atividade a fim de obter implementações de melhorias sempre a um custo justificável.

O fato de o SLM ser considerado a interface entre o a TIC e os Negócios, faz dele um dos processos mais importantes e complexos deste framework.

3.4.5 Gerenciamento de Catálogo de Serviço

O Processo de Gerenciamento de Catálogo de Serviço (SCM - *Service Catalogue Management*) tem como principal objetivo gerenciar as informações contidas dentro do Catálogo de Serviço. Isso inclui compromissos como, por exemplo, garantir que todos os detalhes relativos aos serviços na fase de transição ou operação estejam corretamente ajustados. [15]

O Catálogo de Serviço (*Service Catalogue*) é uma base de dados ou documento que possui informações sobre todos os serviços de TIC que estão sendo prestados, ou prontos para entrar em produção. Ele faz parte do Portifólio de Serviço, especificamente, deve ser usado pela organização no suporte à venda e entrega de serviços. No que tange ao serviço, o catálogo deve possuir informações sobre os relacionamentos "Serviço x Processo de Negócio" e "Serviço x Recursos Técnicos", que geram e suportam o serviço, respectivamente, a fim de gerar conhecimentos necessários para a execução de outros processos (ex: SLM, Gerenciamento da Configuração).

Para descrever o relacionamento entre o Serviço e o Processo de Negócio, existe o Catálogo de Serviço de Negócio (*Business Service Catalogue*), que contém detalhes de todos os serviços entregues ao cliente, incluindo os relacionamentos com as Unidades e Processos de Negócio que dependem desses serviços. Resumidamente, ele é a visão do cliente sobre o Catálogo de Serviço.

Quanto ao relacionamento entre o Serviço e os Recursos Técnicos que o suportam, existe o Catálogo de Serviço Técnico (*Technical Service Catalogue*), que contém detalhes de todos serviços, incluindo os relacionamentos com recursos técnicos - serviços de suporte, serviços compartilhados, componentes e itens de configuração - necessários para suportar a provisão do serviço ao negócio. Estes detalhes devem complementar o Catálogo de Serviço do Negócio, e não fazem parte da visão do cliente.

Dentre os possíveis papéis definidos para este processo, é importante descrever o Gerente do Catálogo de Serviço (*Service Catalogue Manager*), que tem a responsabilidade de manter o Catálogo de Serviço. Isso inclui tarefas como a de garantir que os serviços em operação e em transição estejam registrados no catálogo, sem exceção, e por fim, garantir que essas informações estejam sincronizadas com o Portifólio de Serviço.

3.4.6 Gerenciamento da Disponibilidade

O Processo de Gerenciamento da Disponibilidade apresenta-se importante para a definição de prioridades nos processos da fase operacional, especificamente nos processos de Gerenciamento de Incidentes e Gerenciamento de Problemas. Além destes, o processo de Gerenciamento de Mudanças na fase de transição também utiliza grande parte dos dados gerados por este. [15]

O principal objetivo deste processo é o de produzir (e manter) um Plano de Disponibilidade preciso e atualizado, sempre dependendo das necessidades de negócio, sejam elas atuais ou futuras. É necessário também que a disponibilidade do serviço sempre atenda ou exceda todas as metas acordadas.

Este processo, através de atividades definidas como Reativas e Pró-ativas, contempla aspectos como a disponibilidade do serviço e do componente. Além da Disponibilidade (*Avaliability*) outras medidas dão apoio a este processo, como a Confiabilidade (*Reliability*), Sustentabilidade (*Maintainability*) e a Oficiosidade(*Serviceability*).

A Disponibilidade, em poucas palavras, pode ser definida como a medida do quanto um Serviço ou item de configuração realiza suas funções quando requeridas. Essa medida é determinada pela Confiabilidade, Sustentabilidade, Oficiosidade, Desempenho e Seguraça. O cálculo da Disponibilidade geralmente é feito de forma percentual, baseado no período acordado de disponibilização do serviço e suas respectivas interrupções.

$$Disponibilidade = \frac{(AST - DT) * 100}{AST}$$

A Confiabilidade é definida como o tempo máximo em que o serviço fica disponível sem interrupção. Geralmente, sua medida é feita através do Tempo Médio entre Falhas (MTBF - *Mean Time Between Failures*) e do Tempo Médio entre Incidentes de Serviço (MTBSI - *Mean Time Between Service Incidents*).

A Sustentabilidade pode ser definida como uma medida do quão rápido um Item de Configuração ou Serviço de TIC pode ser recuperado para o trabalho normal após uma falha, e é frequentemente medida como o Tempo Médio para Recuperar Serviço (MTRS - *Mean Time to Restore Service*).

A Oficiosidade é a capacidade de um terceiro cumprir os termos do seu Contrato. Este contrato deve incluir os níveis acordados de Confiabilidade, Sustentabilidade e Disponibilidade para cada item de configuração.

Um conceito importante para este processo é o de Função de Negócio Vital (VBF - *Vital Business Function*), uma função de um Processo de Negócio que é crítica para o sucesso do mesmo. Este conceito apresenta-se importante em vários outros processos, como o de Gerenciamento da Continuidade de Negócio e o Gerenciamento da Continuidade de Serviço de TIC.

Por fim, o Sistema de Informação do gerenciamento da Disponibilidade pode ser apresentado como uma base de dados que contém todos os dados deste processo, usualmente armazenados em múltiplas localizações físicas.

O único papel a ser apresentado é o de Gerente de Disponibilidade (*Availability Manager*),

que tem a responsabilidade de garantir que os objetivos deste processo sejam atingidos, certificando que todos os serviços prestados estejam entregando os níveis de disponibilidade acordados nos SLAs.

3.4.7 Gerenciamento da Capacidade

O Processo de Gerenciamento da Capacidade (*Capacity Management*) tem como principal objetivo a tarefa de garantir que exista capacidade em todas as áreas de TIC a custos justificáveis para antender as necessidades do Negócio acordadas, atuais e futuras, em tempo hábil. Este objetivo deve ser alcançado através da divisão de responsabilidades entre sub-processos, a fim de obter maior precisão partindo de uma abordagem modularizada. [15] Os sub-processos são:

Gerenciamento da Capacidade de Negócio

O Gerenciamento da Capacidade de Negócio (*Business Capacity Management*) é um sub-processo que traduz as necessidades e planos do negócio em termos de requisitos para o serviço e infra-estrutura de TIC, garantindo que os futuros requisitos de negócio para os serviços de TIC sejam quantificados, projetados, planejados e implementados em tempo hábil. Resumidamente, este sub-processo vai fazer com que o serviço que está sendo desenvolvido e o setor de TIC estejam preparados para suprir as possíveis futuras necessidades da área de negócio relacionada.

Gerenciamento da Capacidade de Serviço

O Gerenciamento da Capacidade de Serviço (*Service Capacity Management*) mantém foco no gerenciamento, controle e previsão do desempenho e capacidade fim-a-fim dos serviços em produção, garantindo que o desempenho de todos os serviços, que são detalhados nos SLA e SLR, sejam monitorados e medidos e que os dados coletados sejam registrados, analisados e reportados.

Gerenciamento da Capacidade de Componente

O Gerenciamento da Capacidade de Componente (*Component Capacity Management*) tem como principal objetivo o gerenciamento, controle e previsão do desempenho individual de todos os componentes tecnológicos de TIC, garantindo que todos estes componentes sejam monitorados e medidos, e que os dados coletados sejam registrados e reportados.

Sistema de Informação do Gerenciamento da Capacidade

O Sistema de Informação do Gerenciamento da Capacidade (CMIS - *Capacity Management Information System*) é uma base de dados que suporta o processo de Gerenciamento da Capacidade. Essa base geralmente é armazenada em múltiplas localizações físicas, atendendo aos princípios do processo de Gerenciamento da Continuidade do Serviço de TIC.

Um papel muito importante para este processo é o Gerente de Capacidade (*Capacity Manager*), que tem a responsabilidade de garantir o atendimento dos objetivos do Gerenciamento da Capacidade. Pode-se citar como exemplo a missão de garantir que os recursos de TIC tenham capacidade de atender os objetivos do nível de serviço, e que o uso da capacidade existente seja sempre otimizado. Além disso, este papel deve determinar os requisitos de capacidade de todos os novos serviços, prever requisitos de capacidades futuros a partir de um banco de dados histórico (ou qualquer outro meio possível), manter a validade do Plano de Capacidade e, finalmente, comparar os dados de desempenho em função das SLTs contidas nos SLA.

3.4.8 Gerenciamento de Segurança da Informação

O propósito do processo de Gerenciamento da Segurança da Informação (*Information Security Management* - ISM) é fornecer um foco para todos os aspectos relativos a segurança de TIC na organização, e garantir que esses aspectos sejam efetivamente gerenciados. [15] Para muitas organizações, a segurança só é realizada quando os seguintes objetivos são alcançados:

- Disponibilidade:

  A informação deve estar disponível e utilizável quando for requerido, e os sistemas que a disponibilizam devem ser capazes de resistir a ataques e recuperar-se de (ou prevenir) falhas.

- Confidenciabilidade:

  A informação pode ser observada somente por aqueles que tem o direito de conhecê-la.

- Integridade:

  A informação deve estar completa, correta e protegida contra modificações não autorizadas.

Todos esses aspectos devem ser priorizados no contexto do negócio e dos processos de negócio, uma vez que o gerenciamento só pode definir a segurança dentro do contexto das necessidades do negócio e dos riscos a ele relacionados.

O Sistema de Gerenciamento da Segurança da Informação

O Sistema de Gerenciamento da Segurança da Informação (*Information Security Management System* - ISMS) é uma estrutura que provê uma base para o desenvolvimento de um programa de segurança da informação com efetividade de custo, e que ao mesmo tempo suporte os objetivos do negócio. [15]

O sistema mantém todas as informações que são requeridas pelo ISM em um banco de dados, incluindo todos os controles de segurança, riscos, brechas identificadas e relatórios necessáros para suportar e manter as informações da Política de Segurança e do próprio ISMS.

A ISO 27001 é o padrão de segurança formal no qual as organizações podem procurar a certificação independentemente de seu ISMS, que também pode garantir a obtenção da certificação se desenvolvido e utilizado dentro do modelo de boas práticas pregado pela ITIL®.

O Gerente de Segurança

O Gerente de Segurança tem a responsabilidade de garantir o atendimento dos objetivos do processo em questão. Este conjunto de responsabilidades inclui:

- Assegurar a autorização e o compromisso apropriados da alta gerência de negócios através do desenvolvimento e manutenção das Políticas de Segurança da Informação, além de um conjunto de políticas específicas de suporte.
- Publicar as Políticas de Segurança da Informação a fim de comunicar as partes apropriadas.
- Executar em conjunto com os processos de AM e ITSCM a Análise e o Gerenciamento de Risco.

3.4.9 Gerenciamento da Continuidade de Serviço de TIC

O processo de Gerenciamento da Continuidade de Serviço de TIC (*IT Service Continuity Management* - ITSCM) tem o objetivo de dar suporte ao processo de Gerenciamento da Continuidade de Negócios[1], a fim de garantir a retomada das atividades dos recursos técnicos de TIC e de serviço requeridos no tempo acordado com o negócio. Os recursos técnicos de TIC incluem Sistemas de Computação, Redes, Telecomunicações, e quaisquer outros equipamentos ou programas que suportem o negócio. [15]

[1] O Gerenciamento da Continuidade de Negócios (*Business Continuity Management* - BCM) baseia-se em um conjunto de estratégias e planos de ação com o objetivo de identificar e preservar os serviços essenciais da organização, para que situações imprevisíveis (como por exemplo um incêndio) não destruam as informações mais importantes da mesma.

Resumidamente, o ITSCM é responsável por gerenciar os riscos que podem afetar os serviços de TIC, garantindo que o provedor possa fornecer sempre serviços com o menor risco possível. Para isso, é altamente recomendável que ele seja planejado com o objetivo de suportar o Gerenciamento da Continuidade de Negócio.

Plano de Continuidade do Serviço de TIC

O Plano de Continuidade de Serviço de TIC basicamente define os passos requeridos na recuperação de um ou mais serviços de TIC. Para isso, deve ser realizada a identificação dos gatilhos necessários, tais como a invocação do plano, as pessoas envolvidas, as comunicações e tudo o que for necessário para que este procedimento seja bem sucedido. Vale ressaltar que este plano deve fazer parte integrante do Plano de Continuidade de Negócios.

Análise de Impacto de Negócio

O propósito da Análise de Impacto de Negócio (*Business Impact Assessment* - BIA) é quantificar o impacto referente a perda de um serviço para o negócio, identificando os serviços mais importantes para a Organização, que por sua vez, serão os principais insumos para a definição da estratégia de continuidade.

Gerenciamento de Crise

O Gerenciamento de Crise (*Crisis Management* - CM) é o subprocesso responsável pelo gerenciamento das implicações maiores na continuidade do negócio. No conjunto de responsabilidades da equipe do CM estão:

- O relacionamento com a mídia;
- Manter a confiança dos investidores no negócio;
- Decidir o momento correto de invocar os planos de continuidade de negócio.

Gerente de Continuidade de Serviços de TIC

O gerente do ITSCM é responsável por garantir que os objetivos do processo sejam alcançados. Dentre as atividades sob sua responsabilidade destacam-se:

- A execução da Análise de Impacto nos Negócios, para todo e qualquer serviço, seja ele novo ou já existente;

- Implementar e manter o processo de Gerenciamento da Continuidade de Serviço de TIC, em conformidade com os requisitos gerais do Gerenciamento da Continuidade do Negócio e representar, dentro deste, as funções dos Serviços de TIC;
- Avaliar as questões de continuidade de serviço em potencial e invocar o Plano de Continuidade de Serviço, se necessário;
- Gerenciar o Plano de Continuidade de Serviço enquanto estiver em operação;
- Manter uma programação de teste de TIC, incluindo teste do Plano de Continuidade, alinhado aos requisitos de negócio e sempre após uma mudança num negócio importante.

3.4.10 Gerenciamento de Fornecedor

O processo de Gerenciamento de Fornecedor (*Supplier Management* - SM) deve cuidar basicamente do nível de serviço, bem como monitorar os fornecedores no que tange as condições legais, financeiras, e o preço relacionado ao que é cobrado no mercado, a fim de garantir o valor do investimento realizado. [15]

Base de Dados de Fornecedor e Contrato

A Base de Dados de Fornecedor e Contrato (*Supplier Contract Database* - SCDB) é uma base de dados ou documento devidamente estruturado utilizado para gerenciar os contratos dos fornecedores através do seu ciclo de vida. Contem ainda atributos-chave de todos os contratos com os fornecedores e devem ser parte do SKMS.

Gerente de Fornecedores

O Gerente de Fornecedores é responsável por garantir que os objetivos do processo sejam alcançados. Dentre o seu conjunto de responsabilidades podemos destacar:

- Manutenção e revisão de uma SCDB;
- Revisão e Análise de Risco de todos os fornecedores e Contratos de uma forma regular;
- Monitorar, reportar e rever o desempenho do fornecedor contra os objetivos, identificando melhorias, ações apropriadas e garantir que essas ações sejam implementadas.

Processos da Fase Transição de Serviço

Para a apresentação dos processos desta fase, são necessários alguns conceitos e definições apresentados a seguir:

Conceitos e Definições

Sistema de Gerenciamento do Conhecimento de Serviço

O Sistema de Gerenciamento do Conhecimento de Serviço (*Service Knowledge Management System* - SKMS) é um conjunto de ferramentas e bases de dados utilizados para gerenciar o conhecimento e as informações relativos aos serviços prestados pelo setor. Incluidos na sua arquitetura estão o SCM, SCDB, ISMS, bem como quaisquer outras ferramentas ou bases de dados que armazenem informações relacionadas ao conhecimento adquirido pela organização na prestação de serviços. [15]

A função do SKMS é armazenar, gerenciar, atualizar e apresentar todas as informações que um provedor de Serviços de TIC precisa para gerenciar o Ciclo de Vida dos serviços.

Modelo "V"

É o modelo que define critérios de aceitação para requerimentos estabelecidos de acordo com a fase de desenvolvimento do serviço, relacionando os diferentes níveis de configuração para a construção, teste e validação de acordo com a Especificação dos Requisitos de Serviço, detalhados no Desenho de Serviço.

3.4.11 Gerenciamento de Mudança

O processo de Gerenciamento de Mudança tem a responsabilidade de garantir o registro das mudanças, bem como sua avaliação, autorização, priorização, planejamento, teste, implementação, documentação e revisão de uma maneira controlada. É importante dizer que este processo apenas avalia esses fatores para confirmar a realização dos mesmos, ou seja, o Gerenciamento de Mudança apenas aprova.

Dentro do escopo dessas mudanças estão as alterações nos ativos de serviço e itens de configuração por todo o ciclo de vida do serviço. É importante que a organização defina as mudanças que se encontram fora do escopo deste processo, pois dessa forma, as mudanças com impactos significativamente mais amplos do que as mudanças de serviço[2], e as mudanças de nível operacional[3] podem ser separadas por níveis de equipe, habilidades ou qualquer outro fator que torne este processo suficientemente eficiente para a organização. [15]

Este processo, por sua vez, deve ser planejado em conjunto com os processos SACM e RDM.

[2]Mudanças organizacionais que devam gerar mudanças nos serviços
[3]Reparo a impressoras ou a outros componentes rotineiros do serviço

Tipos de Mudanças

A ITIL® classifica as mudanças a fim de facilitar a organização e o funcionamento deste processo. Dentre os tipos definitos estão: [8]

- **Mudança Normal:**

  É uma mudança complexa, que apresenta riscos desconhecidos e segue procedimentos ou instruções de trabalho não padronizados, como por exemplo, a implementação de um sistema financeiro. Mudanças desse tipo devem ser registradas e rastreadas utilizando-se o mecanismo das *Request For Change* (RFC).[4]

- **Mudança Emergencial:**

  É uma mudança que deve ser implementada o mais rápido possível, como por exemplo a solução de um Incidente grave através da implementação de um pacote de segurança. Normalmente o processo de Gerenciamento de Mudanças possui procedimentos específicos para tratar este tipo de mudança.

- **Mudança Padrão (ou Mudança Simples):**

  É uma mudança pré-aprovada pelo processo, possuindo assim um custo previsto e aprovado, e o risco avaliado. Os procedimentos inerentes a essas mudanças são pré-estabelecidos e já passaram por uma avaliação superior. Por fim, é importante lembrar que algumas mudanças padrão são disparadas pelo processo de Cumprimento de Requisição.

Comitê Consultivo de Mudanças

É um organismo que existe para suportar a autorização das mudanças e auxiliar o Gerente de Mudanças na avaliação e priorização das mesmas. Os membros escolhidos para compor o CAB devem ser capazes de garantir que todas as mudanças dentro do seu escopo sejam adequadamente avaliadas sob o ponto de vista técnico e de negócio.

Comitê Consultivo de Mudança Emergencial

É um sub-conjunto do Comitê Consultivo de Mudança, que avalia e auxilia o Gerente de Mudanças a decidir sobre as mudanças emergenciais de alto impacto para a organização. Os membros deste comitê podem ser convocados no momento em que a reunião deve acontecer em função da natureza da mudança emergencial.

[4] A RFC é uma maneira formal utilizada para realizar pedidos formais para a realização de uma mudança.

Os 7 R's do Gerenciamento de Mudança

São as questões que devem ser respondidas para todas as mudanças. Sem estas informações, a avaliação de impacto não poderá ser completada e o balanceamento entre riscos e benefícios da mudança não poderá ser compreendido. Se os 7 R's não forem considerados, a implementação pode resultar em uma mudança que não entrega todos os benefícios esperados para o negócio, ou ainda, pode entregar resultados indesejados. São eles:

- Quem **requisitou** a mudança?
- Qual é a **razão** para a mudança?
- Qual é o **retorno** requerido da mudança?
- Quais são os **riscos** envolvidos na mudança?
- Quais são os **recursos** envolvidos na mudança?
- Quem é o **responsável** pela construção, teste e implementação da mudança?
- Qual é o **relacionamento** entre esta mudança e outras?

Atividades

O processo de Gerenciamento de Mudança possui várias atividades, citadas a seguir:

- **Criar e registrar a RFC:**

  A mudança é iniciada por uma requisição, e todas as RFCs devem ser registradas e identificadas. É recomendado que esses registros sejam feitos por meio de uma ferrramenta de Gerenciamento de Serviço.

- **Rever a Requisição de Mudança:**

  Esta atividade deve filtrar as requisições, barrando assim submissões incompletas, por exemplo, descrição inadequada, sem necessária aprovação orçamentária. Essas submissões devem, por sua vez, ser retornadas aos emissores.

- **Estimar e Avaliar a Mudança:**

  Dividida em várias etapas, a estimativa e avaliação da mudança deve ser feita primeiramente através da Categorização de Risco, que mede a possibilidade de risco para o negócio de qualquer mudança, onde esta, por sua vez, precisa ser considerada antes da autorização de qualquer mudança.

Tendo a primeira etapa sido concluída, a designação de prioridades se faz necessária, a fim de definir uma ordem cronológica (escalonamento) para a execução das mudanças.

Com a definição do escalonamento de mudanças, a realização do planejamento e programação do conjunto vai assegurar que não haja nenhuma ambigüidade sobre quais tarefas estão incluídas no processo, e ainda assim, é importante desenvolver um Plano de Remediação[5], antes que a mudança seja executada, para endereçar uma falha na mudança ou na liberação.

- **Autorizar a Mudança:**

  Cada mudança deve receber uma autorização formal, fornecida por uma autoridade competente, que pode ser uma pessoa ou um grupo de pessoas. Essa autorização pode ser classificada em níveis, que por sua vez, devem ser julgados pelo tipo, tamanho ou risco da mudança.

- **Coordenar a implementação da Mudança:**

  O processo de Gerenciamento de Mudança tem a responsabilidade de assegurar que as mudanças sejam executadas conforme sua programação. É importante ter em vista que este é um papel de coordenação, enquanto a execução real será de responsabilidade de outros (por exemplo, os técnicos de hardware executarão mudanças de hardware).

- **Revisar e fechar o registro de mudança:**

  Por fim, é necessária uma revisão de mudança (por exemplo, Revisão de Pós-Implementação - PIR) deve ser realizada a fim de confirmar o sucesso da mudança, a satisfação dos *stackholders* e a prevenção de possíveis efeitos colaterais.

Indicadores-Chave de Desempenho - KPI's

Os *Knowledge Performance Indicators* (KPI's) para o Planejamento de Transição e Suporte incluem:

- O número de mudanças implementadas com sucesso.[6]
- Redução da diferença entre escopo, qualidade, custo e tempo atuais e previstos.
- Redução no número de mudanças não autorizadas.
- Redução da quantidade de requisições de mudanças acumuladas.

[5] O Plano de Remediação deve ser utilizado para casos em que a mudança a ser realizada é irreversível. Ele pode, na maioria das vezes, requerer uma revisão da própria mudança no evento da falha, ou ainda ser bastante severo, a ponto de requerer a invocação do Plano de Continuidade da Organização.

[6] São as mudanças que alcançam os resultados acordados em termos de custo, qualidade, escopo, e escalonamento de mudanças.

- Redução do número de mudanças com falhas.

Papéis

- **Gerente de Mudanças:** As principais responsabilidades do Gerente de Mudanças são:
  - Receber, registrar, determinar prioridade e rejeitar RFCs impraticáveis;
  - Planejar as reuniões do CAB;
  - Convocar e presidir reuniões com o CAB e o ECAB;
  - Autorizar mudanças após as reuniões;
  - Publicar programas de mudanças, via Central de Serviço;
  - Rever mudanças implementadas;
  - Fechar RFCs;
  - Produzir relatórios gerenciais;
- **Comitê Consultivo de Mudanças - CAB:**

  É obrigação do comitê participar das reuniões conforme convocação do Gerente de Mudanças; Apoiar o Gerente de Mudanças nas atividades de avaliação, autorização e priorização de mudanças;
- **Comitê Consultivo de Mudança Emergencial - ECAB:**

  Este comitê tem como principal responsabilidade a participação nas reuniões emergenciais conforme convocação do Gerente de Mudanças, bem como o apoio ao mesmo, nas atividades de avaliação, autorização e priorização de mudanças.

3.4.12 Gerenciamento da Configuração e de Ativo de Serviço - SACM

O objetivo do SACM é definir e controlar os componentes (ativos) de serviços e infra-estrutura, a fim de manter com precisão a informação sobre o histórico, o estado corrente e planejado dos mesmos. Neste conjunto de componentes encontram-se versões, baselines, e tudo que possa ser considerado item de configuração. [15]

O Modelo de Configuração

O SACM fornece um modelo de configuração dos serviços, dos ativos e da infra-estrutura, registrando os relacionamentos entre os itens de Configuração. Este modelo, por sua vez, é utilizado em todos os processos do Ciclo de Vida.

Item de Configuração

É chamado de item de configuração qualquer componente que precisa ser gerenciado para garantir a entrega de um Serviço de TIC. Assim, para todo item de configuração as informações relacionadas devem ser registradas no CMS, e o nível de detalhamento varia de acordo com a importância do componente.

Bibliotecas Seguras

Uma biblioteca segura é uma coleção de softwares ou Itens de Configuração documentados com tipos e estados conhecidos. O acesso aos itens, em uma biblioteca segura, é restrito. As bibliotecas são usadas para controle e liberação dos componentes durante todo o Ciclo de Vida do Serviço.

Sistema de Gerenciamento da Configuração

O CMS é um sistema responsável por manter informações sobre os itens de Configuração requeridos na entrega de um Serviço de TIC, incluindo seus relacionamentos. É responsável por manter os relacionamentos entre todos os componentes do serviço e quaisquer documentações de incidentes, problemas, erros conhecidos, mudanças e liberações.

No nível de dados, o CMS pode requerer dados de vários CMDBs físicos, os quais, juntos, serão "plugados" no CMS, assim como as Bibliotecas de Mídia Definitivas.

Depósitos Seguros

Um Depósito Seguro é um local apropriado para armazenar os ativos de TIC. Possui um papel importante na provisão da segurança e continuidade, mantendo confiável o acesso aos equipamentos com a qualidade conhecida.

Sobressalentes Definitivos

É uma área para atendimento local, separada do Depósito Seguro onde deve ser mantido um estoque de sobressalentes de hardware. Esses conjuntos de Sobressalentes podem ser utilizados na recuperação de incidentes ou necessidade de capacidade adicional. Uma vez utilizados temporariamente, retornam ao estoque ou são substituídos.

Linha Base de Configuração - (*Baseline*)

É a configuração de um serviço, produto ou infra-estrutura formalmente revisada e acordada, que desde então serve como base para outras atividades, e que pode ser alterada somente por meio de procedimentos formais de mudança.

Quadro Instantâneo - (*Snapshot*)

É uma "imagem" do estado atual de um item de configuração ou de um ambiente, geralmente capturada por uma ferramenta de descoberta. Este quadro é registrado no Sistema de Gerenciamento da Configuração e permanece como um registro de histórico.

Papéis

- **Gerente de Ativo de Serviço:**

  O Gerente de Ativo de Serviço define políticas e padrões para o gerenciamento de ativos, garantindo a eficiência e efetividade dos Sistemas responsáveis por eles.

- **Gerente de Configuração:**

  O Gerente de Configuração implementa políticas e padrões para o Gerenciamento de Ativo, planeja a população do Sistema de Gerenciamento da Configuração, bibliotecas centrais, ferramentas, códigos e dados comuns, além de garantir a manutenção interna do CMS.

- **Analista de Configuração:**

  O Analista de Configuração cria procedimentos de registro de ICs, controle e privilégios de acesso para o Gerenciamento de Ativo e da Configuração, além de monitorar problemas e manter o banco de dados para coleção e relatório de métricas.

- **Administrador/Bibliotecário de Configuração**

  É o guardião de todas as cópias mestras do software, dos recursos, de CIs, dos ativos e da documentação registrados com os processos de Gerenciamento de Ativo e da Configuração. Dentre as suas responsabilidades principais encontram-se o controle do recebimento, identificação, armazenamento e retirada de todos os CIs suportados, além de fornecer informações sobre o status dos CIs.

- **Administrador do CMS e ferramentas**

  Avalia ferramentas proprietárias de Gerenciamento de Ativos e Configuração e recomenda aquelas que melhor atendam os requisitos orçamentários e técnicos. É responsável

também por customizar diretamente ou indiretamente as ferramentas propretárias para produzir ambientes eficazes de Gerenciamento de Ativos e Configuração, em termos de bases de dados, de bibliotecas de software, de *workflow* e de geração de relatório.

- **Comitê de Controle de Configuração**

  Este comitê é necessário para assegurar que as políticas do Gerenciamento de Configuração estejam empregadas durante todo o Ciclo de Vida do Serviço e com consideração específica para cada aspecto do serviço completo. Definir e controlar as linhas de base da configuração de serviço é um dos seus principais objetivos, a fim de garantir que eles apresentem os requisitos estabelecidos no Desenho de Serviço.

3.4.13 Gerenciamento de Liberação e Implantação

O Gerenciamento de Liberação e Implantação objetiva construir, testar e entregar a capacidade de prover os serviços especificados pelo Desenho de Serviço e que atenderá os requisitos dos interessados (*stakeholders*). [15]

Unidade de Liberação

Uma Unidade de Liberação descreve a porção de um serviço ou infra-estrutura de TIC que é liberada de acordo com a política de liberação da Organização.

Modelos de Liberação e Implantação

Na fase de Desenho de Serviço são definidos os modelos de liberação e distribuição mais adequados, que incluem abordagem, mecanismos, processos, procedimentos e recursos requeridos para construir e distribuir a liberação em tempo hábil e dentro do orçamento.

Biblioteca de Mídia Definitiva

A Biblioteca de Mídia Definitiva - (*Definitive Media Library* - DML) uma ou mais localidades nas quais as versões de todos os Softwares aprovados, licenças e documentação (Itens de Configuração) são seguramente armazenados. Todos os softwares da DML estão sob o controle dos processos de Gerenciamento da Mudança e Gerenciamento de Liberação e Implantação e são registrados no Sistema de Gerenciamento da Configuração. Por fim, somente os softwares vindos da DML serão aceitos para uso em liberações.

Papéis

- **Gerente de Liberação e Implantação**

  É responsável pelo planejamento, desenho, construção, configuração e teste de todo o software e ferramenta para criar o pacote de liberação para a entrega ou para a mudança de um serviço designado.

- **Gerente de Empacotamento e Construção de Liberação**

  Estabelecer a configuração da liberação final, isto é, conhecimento, informação, hardware, software, infra-estrutura, construir e testar a entrega final de liberação.

- **Grupo de Distribuição**

  Entrega física final da implementação do serviço, coordenando a documentação e comunicação de liberação, incluindo treinamento, cliente e Gerenciamento de Serviço.

Processos da Fase Operação de Serviço

3.4.14 Gerenciamento de Incidentes

O processo de Gerenciamento de Incidentes tem como meta primária a restauração da operação normal [7] do serviço o mais rápido possível e minimizar o impacto adverso nas operações do negócio. [11]

Este processo tem autonomia para aplicar uma solução de contorno, mas não para definir uma solução definitiva pois esta deve ser definida pela Gerência de Mudança.

Outro fato importante é a otimização de recursos financeiros obtida através deste processo, uma vez que as pessoas que trabalham nessas tarefas são menos custosas do que as do conselho do Gerenciamento de Problema.

É importante também que o Service Desk possua credibilidade suficiente para que todos os clientes solicitem manutenções através do mesmo, fazendo com que as estatísticas geradas pelo Gerenciamento de Incidentes sejam reais.

Conceitos e Definições

- **Incidente**

  Um incidente é uma interrupção não planejada ou redução na qualidade de um Serviço de TIC. A falha de um Item de Configuração que ainda não afetou o Serviço de TIC poderá gerar um incidente.

[7] A "Operação Normal" do serviço é definida como a operação dentro dos limites estabelecidos nos SLA.

- **Impacto**

  É a medida do efeito de um incidente, problema ou mudança nos processos de Negócios. O impacto é sempre baseado em como os níveis de serviço serão afetados.

- **Urgência**

  É uma medida de quão longo será o tempo até que um Incidente, Problema ou Mudança tenha um impacto significativo para o Negócio.

- **Prioridade**

  É uma categoria utilizada para identificar a importância relativa de um Incidente, Problema ou Mudança. A prioridade deve ser baseada no Impacto e Urgência e é utilizada para identificar os tempos requeridos para a realização das respectivas ações.

- **Solução de Contorno**

  É a redução ou eliminação do impacto de um Incidente ou Problema no qual a resolução completa ainda não está disponível. Essas soluções, no caso em que os incidentes não possuem registros de problemas associados devem ser documentadas nos registros de incidentes. Por último, as Soluções de Contorno para problemas devem ser documentadas nos registros de Erros Conhecidos.

- **Prazos para execução e escalonamento**

  Prazos de execução precisam ser acordados para todos os estágios de tratamento de incidentes (que irão diferir de acordo com a prioridade do incidente) baseados nos objetivos de resolução previstos em SLA, OLA e UC.

- **Modelo de Incidente**

  Um Modelo de Incidente é uma forma de pré-definir os passos que devem ser seguidos para tratar um incidente. Para isto, ferramentas de suporte podem ser utilizadas como meio de gerenciamento do processo requerido. Esses modelos devem definir os passos a serem executados em ordem cronológica, responsabilidades, tempos de execução, procedimentos de escalonamento e geração de evidências, a fim de garantir que todas as medidas cabíveis sejam tomadas.

- **Incidente Grave**

  É a maneira como são classificados incidentes que provocam alto impacto sobre o negócio. Esses inicidentes requerem procedimentos específicos, menor prazo de execução e maior urgência. A definição do que constitui um incidente grave precisa ser acordada e mapeada no mecanismo de priorização de incidente.

Atividades

Este processo prevê um conjunto de atividades a fim de gerenciar com eficiência os incidentes ocorridos dentro da organização. São elas:

- Identificar Incidente
- Registrar Incidente
- Categorizar Incidente
- Priorizar Incidente
- Diagnosticar Inicialmente
- Escalonar Incidente
- Investigar e Diagnosticar
- Resolver e Recuperar
- Fechar Incidente

Gerenciar os incidentes é uma tarefa chave para cumprir os SLAs com eficiência e baixo custo.

Indicadores-Chave de Desempenho

Os KPI's devem ser utilizados a fim de avaliar os resultados obtidos através da execução deste processo. Além disso, eles são de extrema importância na elaboração da melhoria contínua.

- Quantidade total de incidentes.
- Avaliação dos incidentes em cada estágoio.
- Quantidade de incidentes abertos e não resolvidos.
- Número e porcentagem dos incidentes principais.
- Tempo Médio decorrido para conseguir a resolução ou contorno, quebrado por código de impacto.
- Porcentagem de incidentes manuseados dentro do tempo de resposta acordado.

Papéis

- **Gerente de incidentes**

  Dentre as responsabilidades deste papel, podemos citar a de desenvolver e manter todas as etapas deste processo, desta forma, garantindo a eficiência e efetividade do processo de Gerenciamento de Incidente. Produzir informações gerenciais, desenvolvier e manter Sistemas de Gerenciamento de Incidente, e gerenciar incidentes graves.

- **Suporte de Primeiro Nível**

  Este papel é de extrema importância, pois resolve incidentes de baixa complexidade em primeira instância, reduzindo assim a sobrecarga sobre os técnicos responsáveis por incidentes de maior importância.

Desafios

Uma boa Central de Serviço é a chave do sucesso para o Gerenciamento de Incidentes.

3.4.15 Gerenciamento de Eventos

O Gerenciamento de Eventos é um processo focado na geração e detecção de notificações significativas a respeito do estado da infra-estrutura e Serviços de TIC. O conceito de monitoração, muitas vezes confundido com o Gerenciamento de Eventos, pode ser exemplificado por ferramentas que monitoram o estado de um dispositivo para garantir que ele esteja operando dentro dos limites aceitáveis, mesmo que aquele dispositivo não esteja gerando eventos. [11]

Um evento é uma mudança de estado que tem significado para o gerenciamento de um Item de Configuração ou Serviço de TIC. Este termo também pode ser utilizado para identificar um alerta ou notificação criado por qualquer Serviço de TIC, Item de Configuração ou ferramenta de Monitoração. Eventos, tipicamente requerem profissionais de Operação de TIC na tomada de decisões e frequentemente requerem a abertura e registro de Incidentes.

Tipos de Eventos

Os eventos devem ser classificados, a fim de facilitar a análise dos mesmos. Os tipos mais comuns utilizados na classificação de eventos são:

- Eventos que significam uma operação regular *(Informational)*;

  Ex: Login de um usuário.

- Eventos que significam uma exceção *(Excpeption)*;

  Ex: Consumo de banda além do comum por uma máquina da rede.

- Eventos que significam uma operação não usual, porém não são exceções *(Warning)*;

  Ex: Consumo de memória acima do esperado por um breve espaço de tempo.

Papéis

Não é usual existir um Gerente de Eventos, uma vez que as atividades deste processo normalmente são desempenhadas por software e dispositivos de monitoramento.

3.4.16 Cumprimento de Requisição

Os objetivos deste processo envolvem o fornecimento de um canal para os usuários solicitarem e receberem serviços-padrão, onde para os quais existe uma aprovação pré-definida e processo de qualificação. Além disso, dar assistência com informação geral, reclamação ou comentários, distribuir componentes de serviços (ex: Licenças de Software), e prover qualquer tipo de informação que de alguma forma seja necessária para estes. [11]

Conceitos e Definições

Requisição de Serviço

Uma requisição de usuário por informações, aconselhamento, mudança padrão ou acesso a um Serviço de TIC. Essas requisições são geralmente tratadas pela Central de Serviço e não requerem a submissão de uma RFC.

Modelos de Requisições

Requisições de Serviço ocorrem frequentemente e requerem seu atendimento através de uma maneira consistente, de forma a atender os níveis de serviço acordados. Para dar assistência a essas solicitações, muitas Organizações criam Modelos de Requisições pré-definidos, os quais tipicamente incluem alguma forma de pré-aprovação por parte do processo de Gerenciamento de Mudança).

3.4.17 Gerenciamento de Problema

O principal objetivo deste processo é previnir a ocorrência de problemas e dos incidentes resultantes, bem como eliminar a recorrência de incidentes. essas duas ações são classificadas

pela ITIL® como Pró-ativas e Reativas, respectivamente. Ademais, é importante que o impacto dos incidentes que não podem ser previnidos seja minimizado. [11]

Conceitos e Definições

Problema

Um problema é a causa não conhecida de um ou mais Incidentes. Essa causa não é conhecida no momento que o registro do problema é criado e o processo Gerenciamento de problema é responsável pelas investigações adicionais.

Erro Conhecido

É um problema que possui a sua causa-raiz identificada e uma solução de contorno documentada. Erros conhecidos são criados e gerenciados através de seu ciclo de vida pelo Gerenciamento de Problema.

Modelos de Problemas

Muitos problemas são únicos e devem receber tratamento individual, porém alguns incidentes podem ocorrer novamente devido a problemas não identificados. Este conceito é similar ao conceito de Modelos de incidentes já descritos no processo de Gerenciamento de Incidente.

Base de Dados de Erros Conhecidos

O propósito dessa base de dados é permitir o armazenamento de conhecimentos prévios a respeito de incidentes e problemas (e como eles foram superados), possibilitando diagnóstico e resolução rápidos, caso voltem a ocorrer. O Registro de Erro Conhecido deve reter todos os detalhes da falha ocorrida e seus respectivos sintomas, juntamente com detalhes de qualquer solução de contorno ou ação de resolução que venha a ser realizada para solucionar incidentes ou problemas.

Papéis

Gerente de Problemas

As responsabilidades deste papel incluem:

- Contato constante com os grupos de resolução de problemas, para garantir rápida resolução dentro dos objetivos dos Acordos de Nível de Serviço.
- Proprieade e proteção do Banco de Dados de Erros Conhecidos.

- Responsável pela inclusão de todos os erros conhecidos no Banco de Dados de Erros Conhecidos e algoritmos de pesquisa.
- Fechhamento formal de todos os registros de problema.
- Contato com fornecedores e contratados, para garantir que os terceiros cumpram com suas obrigações contratuais, no que diz respeito a resolução de problemas.
- Arranjar, executar, documentar todas as atividades relacionadas às Revisões de Problemas Graves.

Grupos de Soluções de Problemas

São os grupos técnicos de suporte (interno ou de provedores) coordenados pelo Gerente de Problemas.

3.4.18 Gerenciamento de Acesso

O objetivo deste processo é garantir aos usuários autorizados o direito de usar um serviço, enquanto impede tal acesso aos usuários não autorizados. O processo corresponde à execução de políticas e ações definidas nos processos de Gerenciamento de Segurança e Gerenciamento da Disponibilidade. [11]

Conceitos e Definições

Acesso:

Refere-se ao nível e extensão da funcionalidade de um serviço ou dado que é permitido a um usuário utilizar.

Identidade

Refere-se a informação sobre o usuário, que o distingue dos demais e que demonstra sua situação dentro da Organização. Por definição, a identidade de um usuário é exclusiva.

Direitos ou Privilégios

Referem-se a regulamentação definida, que determina o acesso a ser oferecido ao usuário para um serviço ou grupo de serviços. Os direitos típicos (ou níveis de acesso) incluem leitura, gravação, execução, alteração e remoção.

Serviços ou Grupo de Serviços

Usuários não usam somente um serviço e usuários que executam um conjunto de atividades similares podem usar um conjunto similar de serviços. Ao invés de providenciar acesso

individual para cada serviço, é mais eficiente conceder a um grupo de usuários o acesso completo aos serviços que eles estão habilitados a usar.

Serviços de Diretório

Refere-se a um tipo específico de ferramenta que é utilizada para gerenciar o acesso e direitos dos usuários.

Processos da Fase Meloria de Serviço Continuada

Conceitos e Definições:

Premissas soobre Medição e Gerenciamento [18]

- É impossível gerenciar o que não se pode controlar.
- É impossível controlar o que não se pode medir.
- É impossível medir o que não se pode definir.

Plano de Melhoria de Serviço

Um plano formal para implementar melhoria em um processo ou serviço de TIC, relacionado com o SLM.

Retorno do Investimento - ROI

Uma medida do benefício esperado de um investimento. No senso mais simples é o lucro líquido de um investimento dividido pelo valor líquido dos ativos investidos.

Valor do Investimento - VOI

Uma medida do benefício esperado de um investimento. O VOI considera benefícios financeiros e benefícios intangíveis.

Gerenciamento de Conhecimento

Esta atividade possui um papel central na Melhoria Contínua do Serviço. Considerando os dados gerados através dos processos nas fases anteriores, é feita uma análise a fim e gerar informação, que por sua vez, vai gerar conhecimento sobre a organização.

Princípios e Modelos-Chave

Modelo PDCA O ciclo ***P**lan, **D**o, **C**heck, **A**ct* (Planejar, Executar, Conferir e Atuar), possui uma significativa contribuição na busca de alta qualidade, aumento de produtividade e uma

melhor posição competitiva. W. Edwards Deming é bastante conhecido por esta filosofia de gerenciamento. Após estes estágios existe uma fase de consolidação que objetiva evitar que se retorne à situação original.

A ITIL® prega que este ciclo deve ser efetuado continuamente, a fim e manter o nível de maturidade alcançado. Uma descrição mais detalhada das ações são apresentadas a seguir:

- **Planejar** Estabelecer metas para melhoria, incluindo a análise de *gap* e definições para sua eliminação com a impementação de medidas para garantir que os benefícios sejam alcançados.
- **Executar** Desenvolver e implementar um projeto para eliminar os *gaps*.
- **Verificar** Determinar se um *gap* ainda existe em relação às medidas de sucesso estabelecidas na fase do Plano. Este *gap* pode ser considerado tolerável se o desempenho atual está dentro dos limites de performance permitidos.
- **Atuar** É o processo de decisão para determinar se há mais atividades requeridas para eliminar *gaps* remanescentes. Decisões do Projeto nesse estágio são a entrada para a próxima etapa do ciclo de vida.

Modelo de Melhoria de Serviço Continuada

Muitas oportunidades de melhoria de serviços podem ser sumarizadas em seis etapas:

- Adotar uma visão compreendendo os objetivos de alto nível do Negócio. A visão deve ainhar as estratégias de TIC e do Negócio.
- Avaliar a situação atual em termos do Negócio, da Organização, das pessoas, do processo e da tecnologia.
- Compreender e definir um acordo sobre as prioridades para melhoria, baseado nos princípios definidos na visão.
- Detalhar o Plano de Melhoria do Serviço (SIP) para alcançar uma mehor qualidade na entrega de serviços pela impementação dos processos de Gerenciamento dos Serviços de TIC.
- Verificar quais medidas e métricas sao aplicadas para garantir que os marcos sejam alcançados, para que os processos estejam em conformidade e que os objetivos e prioridades do Negócio sejam atendidos pelos níveis de serviço estabelecidos.
- O processo deve garantir que o impulso para a mehoria da qualidade seja mantido, assegurando-se que mudanças se tornem parte da cultura da organização.

Valor para o Negócio Basicamente, existem 4 razões pelas quais são realizados monitoramentos e medições. São elas:

- **Validar:** Vaidar decisões prévias.
- **Direcionar:** Direcionar um conjunto de atividades sequenciais para atingir um objetivo.
- **Justificar:** Justificar, com uma evidência ou prova, sobre a necessidade de ações.
- **Intervir:** Identificar ações corretivas.

Linha de Base - *Baseline* Uma Linha de Base é uma marca inicial estabelecida para comparação posterior. São utilizadas para estabelecer um ponto inicial e determinar se um processo ou serviço precisa de melhoria. Existe, para todas elas, a importância de documentação, reconhecida e aceita através da Organização. Linhas de Base são utilizadas também para medir a efetividade de um SIP.

Tipos de Métricas

- **Métricas de Tecnologia** São metricas associadas a componentes ou aplicações, como por exemplo, disponibilidade e desempenho.
- **Métricas de Processo** São métricas que determinam a "saúde" do processo. Essas métricas são representadas na forma de Fatores Críticos de Sucesso, KPIs e métricas de atividade relativas a um processo.
- **Métricas de Serviço** As métricas de serviço são simplesmente os resutados apresentados por este, fim-a-fim. Elas são compostas por métricas de processos, que por sua vez, são capazes de fornecer valores tangíveis de avaliação.

KPIs

A ITIL® recomenda que nos estágios preliminares de um programa de Melhoria Contínua do Serviço somente dois ou três KPIs para cada CSF sejam definidos, monitorados e reportados. Depois de um decorrer de tempo, esses indicadores podem realizar mudanças, baseadas no que é importante para o negócio e no gerenciamento de TIC. A partir disso, o próximo passo é identificar as métricas e medidas requeridas para computar cada KPI, seja ele quantitativo ou qualitativo[8].

[8] O tipo do KPI está diretamente relacionado com a CSF. Por exemplo:

- Melhorar a qualidade do Serviço de TIC.
- Reduzir custos de TIC.

3.4.19 Processo de Melhoria dos Sete Passos

Este processo foi desenvolvido sob o conceito de que a CSI é fundamentada em medições, objetivando reduzir *gaps*. [12] Desta forma, o Processo de Melhoria dos Sete Passos é descrito a seguir:

1. **Definir o que deve ser medido.**

   Os processos das fases de Estratégia e Desenho de Serviço devem identificar o que deve ser medido.

2. **Definir o que pode ser medido**

   Relaciona as atividades de CSI dos objetivos almejados pela identificação dos requisitos do novo nível de serviço do negócio, as capacidades de TIC (identificadas na Transição de Serviço) e os orçamentos disponíveis. O processo de CSI pode conduzir a análise de *gap* para identificar as oportunidades para melhoria respondendo a questão de como chegar ao objetivo almejado.

3. **Coletar os dados**

   Os dados são reunidos baseados em metas e objetivos identificados, de forma a responder adequadamente se o setor chegou ao ponto que os líderes queriam. Os dados são coletados na Operação de Serviços.

4. **Processar os dados**

   Os dados são processados em alinhamento com os CSFs e os KPIs especificados. Uma vez que os dados tenham sido racionalizados, a análise pode ser inicada.

5. **Analisar os dados**

   Nesta fase os dados se tornam informação identificando *gaps* de serviço, tendências e impacto do negócio.

6. **Apresentar e usar da informação**

   É a apresentação e informação de um quadro exato dos resultados e esforços de melhoria aos principais interessados (*stakeholders*), dando a capacidade de responder se os objetivos serão alcançados, por exemplo.

7. **Implementação de ação corretiva**

Os itens citados anteriormente são CFSs. O primeiro resultaria em um KPI qualitativo, como por exemplo, aumentar em uma determinada porcentagem a satisfação dos clientes em relação ao tratamento de incidentes. O segundo, por sua vez, resultaria em um KPI quantitativo, como por exemplo, reduzir em uma determinada porcentagem os custos no tratamento de incidentes em impressoras.

São as ações que necessitam ser implementadas para melhorar o serviço, sendo comunicadas e explicadas para a Organização. A partir desta etapa, a Organização estabelece uma nova linha de base e o ciclo recomeça.

O conhecimento adquirido é usado para otimizar, melhorar e corrigir os serviços.

Integração do Gerenciamento do Nível de Serviço com a Melhoria de Serviço Continuada

A adoção do SLM é um princípio-chave da CSI. O SLM suporta o Processo de Melhoria dos Sete Passos determinando o que medir, definindo requisitos de monitoração, reportando os níveis e serviços alcançados.

Essas medidas são possíveis uma vez que o SLM trabalha com a área de negócio para compreender novos requisitos de serviço ou mudanças em serviços existentes. Isso, por sua vez, gera entradas para as atividades de CSI e ajuda a priorizar projetos de melhoria.

Papéis

Gerente de Melhoria de Serviço Continuada

É o responsável pelo sucesso de todas as atividades do CSI. Suas amplas responsabilidades requerem competência e que um alto nível de autoridade[9] lhe seja concedido.

3.5 Funções

3.5.1 Central de Serviços

A Central de Serviços é uma das principais funções utilizadas pela ITIL®. Ela serve como meio de contato para os usuários dos serviços fornecidos a fim de resolver problemas, efetuar requisições de serviços, pedir informações, e até para algumas categorias de requisições de mudança [11].

Segundo a ITIL®, existem três tipos mais utilizados de Central de Serviços:

- **Central de Serviços Local:**

  A Central de Serviços Local é implementada para atender necessidades e cada unidade de negócio dentro da organização, de modo que são criadas várias centrais, uma para cada unidade. Esse tipo de abordagem deve ser usado somente quando há necessidades

[9] Importante para que as competências comportamentais sejam efetivas, uma vez que um gerente deste processo sem autoridade não conseguiria manter a disciplina necessária para a melhoria contínua.

específicas em cada unidade de negócio, fazendo com que o atendimento seja facilitado pois a equipe de suporte já esta implementada no local. É incomum que o custo operacional para este tipo de abordagem seja maior, pois será montada uma estrutura (software/hardware) para cada área de negócio dentro da organização.

- **Central de Serviços Centralizadas:**

  A Central de Serviços Centralizada deve atender todas as areas de negócio dentro da organização. Isso ocasiona na redução de custos e na otimização na utilização e gerenciamento dos recursos.

- **Central de Serviços Virtual:**

  No caso de empresas multinacionais, a Central de Serviços Virtual pode ser uma boa opção, pois ela não precisa de uma localização geográfica definida. Apenas é definido um ponto central de contato (telefone/web), e a partir disso o usuário comunica-se com a central que fala seu idioma, ou que funciona no horário que ele necessita.

3.5.2 Gerenciamento Técnico

Tem o objetivo de apoiar o planejamento, implementação e manutenção da infra-estrutura técnica para suportar os Processos de Negócio, através de topologias técnicas resilientes, utilização adequada do conhecimento técnico para manter a infra-estrutura em condições, e por fim, o pronto uso deste conhecimento a fim e diagnosticar rapidamente qualquer falha que venha a ocorrer. [11]

As equipes devem ser agrupadas de acordo com seu conhecimento técnico determinado pela tecnologia a ser gerenciada, por exemplo, equipes de *Mainframe*, Servidores, *Storage* e Rede.

3.5.3 Gerenciamento de Operações de TIC

Objetiva a manutenção do *"status quo"*[10] para atingir a estabilidade das atividades e processos do dia-a-dia. Para isso, realiza constante análise e melhoria a fim e obter aperfeiçoamento dos serviços e redução de custos, com a manutenção da estabilidade, baseada em padrões de desempenho definidos durante a fase de Desenho de Serviço. [11]

[10] É uma expressão latina que designa o estado atual das coisas, seja em que momento for.

3.5.4 Gerenciamento de Aplicação

Tem a função de suportar os processos de negócio ajudando na identificação funcional dos requerimentos de aplicação e então apoiar o desenho, transição, operação e melhoria destas. [11]

4 *ITIL® V3 x COBIT® 4.1*

A crescente adoção das melhores práticas para Governança e Gerenciamento de Serviços de TI apresentadas nos capítulos anteriores, são fruto da necessidade do setor de gerenciar a qualidade e a confiabilidade dos seus negócios, e desta forma, ser capaz de responder ao grande número de requisitos regulamentadores e contratuais da atualidade. No entanto, existe um grande risco relacionado à implementação destas práticas, uma vez que se elas forem tratadas como um guia puramente técnico, elas podem tornar-se custosas e desfocadas. Para que sejam mais efetivas, as melhores práticas devem ser aplicadas dentro do contexto do negócio, mantendo o foco onde o seu uso pode fornecer maiores benefícios à organização.

Neste capítulo será apresentado o alinhamento entre os *frameworks* COBIT® e ITIL®. O primeiro, apesar de ser orientado a processos é um *framework* de controle global, e desta forma, apresenta apenas **o que** deve ser feito para se obter uma Governança de TI efetiva, e não **como** isso deve ser feito. O segundo, define melhores práticas para o gerenciamento de serviços de TI através de processos com passos detalhados, ao invés de definir um *framework* de controle global. Assim, este alinhamento objetiva proporcionar uma visão precisa para a Governaça de TI no que tange o Gerenciamento de Serviços, relacionando a superficialidade dos processos e objetivos de controle do COBIT®, com o aprofundamento dos processos do ITIL®.

4.1 A Estratégia de Serviços e o COBIT®

Os fundamentos da Estratégia de Serviços apresentados pelo primeiro livro da biblioteca ITIL® tratam de questões como, por exemplo, a tomada da estratégia como uma perspectiva[1], uma posição[2], um plano[3] e finalmente, um padrão[4]. O PO1 é processo do COBIT® relacionado

[1] Define-se um conjunto regente de crenças e valores compartilhados por toda a organização. A perspectiva configura a direção global na qual o provedor de serviços se move a fim de alcançar seus objetivos, e construir sua anatomia de performance.

[2] A estratégia tomada como uma posição é interpretada como um diferencial na mente dos consumidores. Isto normalmente significa competir no mesmo espaço que as outras empresas do ramo, com uma proposição de valor diferenciada que é atrativa ao cliente.

[3] É um modo de agir, indo de um ponto a outro, dentro de um cenário competitivo. Frequentemente referenciado como estratégia pretendida, é o modo de ação deliberado, traçando um caminho através dos objetivos estratégicos.

[4] Os padrões estão embutidos na maneira em que o provedor faz negócio.

a esses fundamentos, uma vez que ele requer a definição de um plano estratégico de TI que traduza os requisitos de negócio em ofertas de serviço, para que, finalmente, esses serviços sejam entregues de uma forma transparente e efetiva.

4.1.1 O Gerenciamento Financeiro e o COBIT®

O processo de Gerenciamento Financeiro de TI, responsável por quantificar o valor dos serviços em termos financeiros, pode ser utilizado para atender os seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO1:** O Gerenciamento do Valor de TI;
2. **PO5:** O *Framework* de Gerenciamento Financeiro;
3. **DS6:** A contabilização e a modelagem de custo.

Todos esses requisitos são trabalhados pelo processo de Gerenciamento Financeiro (seção 3.4.3). O Gerenciamento do Valor de TI é atendido pela Análise de Investimento, que tem a função de produzir valor ao longo do ciclo de vida do serviço a partir da quantia recebida, bem como dos riscos incorridos. O *framework* de Gerenciamento Finaiceiro, a contabilização e a modelagem de custo, são atendidos pelos sub-processos: contabilização, cobrança, e caso de negócio, que devem gerenciar a variação do orçamento, alocar e distribuir custos, e dar suporte às decisões, respectivamente.

4.1.2 O Gerenciamento da Demanda e o COBIT®

O processo de Gerenciamento da Demanda **??** objetiva influenciar a chegada de demanda na organização, a fim de facilitar as tarefas do processo de Gerenciamento da Capacidade. Desta forma, ele pode atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO1:** O Plano Estratégico de TI;
2. **PO8:** O Foco no Cliente através do Gerenciamento da Qualidade;
3. **DS1:** A definição dos Níveis de Serviço.

Os requisitos 1 e 2 são parcialmente atendidos. O primeiro, deve utilizar a demanda como um ativo estratégico que pode ser influenciado, e o segundo, é fortemente utilizado para que se possa analisá-la precisamente. Em ambos os casos, o nível de relacionamento entre esses requisitos e o processo vai depender do tipo de estratégia tomada pela gerência. O requisito

3 é altamente influenciado pelo Gerenciamento da Demanda. Essa influência é dada pelo fato de a definição dos níveis de serviço depender da capacidade da organização, que por sua vez, depende da demanda proporcionada. Desta forma, o Gerenciamento da Demanda vai influenciar indiretamente na definição dos níveis de serviço.

4.1.3 O Gerenciamento do Portfólio de Serviço e o COBIT®

O processo de Gerenciamento do Portfólio de Serviço descreve os serviços de um provedor na perspectiva de valor de negócio. Assim, ele pode atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO1:** O Gerenciamento de Portfólio;
2. **PO4:** Priorizar os recursos, de acordo com a necessidade;
3. **PO5:** O Gerenciamento de Investimento;
4. **DS1:** Definir e Gerenciar níveis de serviço;
5. **DS6:** A Definição dos Serviços com relação aos custos.

Como visto na seção 3.4.1, o processo de Gerenciamento do Portfólio de Serviço atende a todos os requisitos apresentados anteriormente exceto o 4, que é apenas influenciado por este processo[5]. Os requisitos 2, 3 e 5 são possíveis devido à visão abrangente com relação a todos os serviços prestados dentro deste processo.

Esta influência acontece a partir da relação entre a demanda e a capacidade da organização, e da relação entre a capacidade e o gerenciamento de nível de serviço. A demanda define a capacidade, da qual os níveis de serviço dependem. Assim, este processo pode influenciar os níveis de serviço a fim de favorecer os serviços que possuirem maior demanda ou valor comercial, por exemplo.

Por fim, foi verificado que a fase de Estratégia de Serviço do ITIL® possui forte relacionamento com os processos do domíno de Planejamento e Organização, e também de Entrega e Suporte do COBIT® citados anteriormente.

4.2 O Desenho de Serviço e o COBIT®

O objetivo da fase de Desenho de Serviço do ITIL® é produzir o desenho de processos que atendam as necessidades de negócio, e que possam ser operados e melhorados em ambientes

[5]Por exemplo, nas organizações que utilizam vários níveis de acordos e contratos, os serviços ja nascem diretamente ligados aos níveis de serviço

seguros. Os requisitos dos processos PO4 e DS1 do COBIT® estão diretamente relacionados a estes objetivos, pela necessidade de definir os processos da organização e o gerenciamento de níveis de serviço, respectivamente.

4.2.1 O Gerenciamento do Catálogo de Serviços e o COBIT®

Este processo deve criar e manter o catálogo de serviços, garantindo que este contenha informações precisas e atualizadas. Desta forma, este processo é capaz de atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO4:** Um *framework* de processos de TI que garanta transparência e controle;
2. **DS1:** A definição dos serviços.

Como visto na seção 3.4.5, o processo de Gerenciamento do Catálogo de Serviços atende completamente os requisitos apresentados. Quanto ao requisito número um, gerenciar o catálogo garante transparência e controle no que tange serviços de TI.

4.2.2 O Gerenciamento de Nível de Serviço e o COBIT®

Este processo negocia e documenta metas de serviço apropriadas com o negócio, e a partir disso, gera relatórios com relação a performance através do monitoramento. Assim, este processo é capaz de atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO4:** Definir os relacionamentos entre o setor de negócios e o de TI;
2. **PO8:** Obter melhoria contínua de processos;
3. **AI5:** Gerenciar os contratos com fornecedores;
4. **DS1:** Gerenciar os níveis de serviço;
5. **DS2:** Gerenciar serviços de terceiros;
6. **ME1:** Obter dados através de monitoramento, e avaliar a performance.

Esses requisitos, com excessão do requisito numero dois, são totalmente atendidos pelo processo de Gerenciamento de Nível de Serviços apresentado na seção 3.4.4. O requisito número dois é parcialmente atendido, uma vez que este processo apenas gera informações para que, na fase de melhoria contínua, este requisito seja totalmente atendido.

O requisito número 1 é atendido a partir dos Acordos de Nível de Serviço, os números 3 e 5 através dos contratos estabelecidos, e o número 6 é atendido por todo o processo, uma vez que é necessário monitorar as atividades realizadas a fim e garantir que elas estão de acordo com os termos acordados.

4.2.3 O Gerenciamento da Capacidade e o COBIT®

Este processo deve garantir que uma capacidade de custo justificado exista em todas as áreas do setor de TI, para que assim, seja possível alcançar as metas de negócio acordadas dentro de um limite de tempo aceitável. Desta forma, este processo é capaz de atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **PO3:** Definir uma direção tecnológica para suportar o negócio;
2. **AI1:** Definir e manter os requisitos funcionais de negócio;
3. **DS3:** Gerenciar a performance e a capacidade;
4. **DS13:** Reduzir os atrazos de negócio e os custos de operações de TI.

Como visto em 3.4.7, todos esses requisitos são atendidos pelo processo de Gerenciamento da Capacidade. No requisito número 1, a direção tecnológicas são as tecnologias de infra-estrutura que irão suportar o negócio.

4.2.4 O Gerenciamento da Disponibilidade e o COBIT®

O Gerenciamento da Disponibilidade deve fazer com que todos os serviços atinjam as SLTs a um custo justificável. Assim, ele é capaz de atender aos seguintes requisitos apresentados pelos processos do COBIT®:

1. **DS3:** Manter a disponibilidade dos recursos;
2. **DS4:** Garantir continuidade, sustentabilidade e a confiabilidade dos serviços.

Ambos os requisitos são completamente atendidos pelo processo, conforme foi verificado na seção 3.4.6.

4.2.5 O Gerenciamento da Segurança da Informação e o COBIT®

Este processo alinha a segurança de TI com a segurança do negócio, garantindo uma gerência efetiva de todos os serviços e, ao mesmo tempo, atendendo aos padrões determinados pela ISO 27001. Assim, este processo tem plenas condições de atender aos seguintes requisitos:

1. **AI3:** Proteção e disponibilização dos recursos de infra-estrutura;
2. **DS5:** Gerenciar a segurança de TI e definir um programa de segurança.

Como visto em 3.4.8, ambos os requisitos são atendidos completamente.

4.2.6 O Gerenciamento de Fornecedores e o COBIT®

Este processo gerencia os fornecedores e os serviços a eles terceirizados, a fim de garantir o ROI e a qualidade dos serviços de TI ao negócio. Desta forma, este processo é capaz de atender os seguintes requisitos de processos do COBIT®:

1. **AI5:** Gerenciar contratos com fornecedores;
2. **DS2:** Monitorar a performance dos fornecedores.

Ambos os requisitos são completamente atendidos pelo processo, conforme foi verificado na seção 3.4.10.

4.2.7 O Gerenciamento da Continuidade do Serviço de TI e o COBIT®

O processo de Gerenciamento da Continuidade do Serviço de TI suporta a continuidade do negócio com o objetivo de garantir a sustentabilidade dos serviços de TI. Assim, este processo é capaz de atender os seguintes requisitos de processos do COBIT®:

1. **PO9:** Estabelecer um *framework* para o gerenciamento de riscos;
2. **AI1:** Apresentar um relatório de análise de riscos;
3. **DS4:** Gerenciar a Continuidade dos Serviços.

Como visto na seção 3.4.9, todos esses requisitos são completamente atendidos por este processo.

4.2.8 O Gerenciamento da Mudança e o COBIT®

Este processo deve maximizar as chances de sucesso das mudanças realizadas no setor de TI, e ao mesmo tempo, minimizar os riscos inerentes a elas. Desta forma, este processo é capaz de atender o seguinte requisito de processo do COBIT®:

1. **AI6:** Gerenciar Mudanças.

O requisito acima é completamente atendido pelo processo de Gerenciamento de Mudanças, cujos detalhes foram apresentados na seção 3.4.11.

4.2.9 O Gerenciamento da Configuração e de Ativo de Serviço e o COBIT®

Este processo suporta o controle e o gerenciamento de ativos de serviço. Desta forma, este processo é capaz de atender ao seguinte requisito de processo do COBIT®:

1. **DS9:** Gerenciar a Configuração.

O gerenciamento requisitado acima é realizado com efetividade pelo processo, que é detalhado na seção 3.4.12.

4.2.10 O Gerenciamento de Liberação e Implantação e o COBIT®

Este processo responsabiliza-se por construir, testar e entregar a capacidade de prover os serviços, que atenderá os requisitos dos *stakeholders*. Assim, este processo é capaz de atender aos seguintes requisitos de processo do COBIT®:

1. **PO8:** Um sistema de gerenciamento da qualidade.
2. **AI3:** Um ambiente de tesde de viabilidade.
3. **AI4:** Disseminar todas as formas de conhecimento com relação a novos sistemas.
4. **AI7:** Instalar e credenciar soluções, oferecer um ambiente de teste e realizar revisões de pós-implementação.

O requisito número um é parcialmente atendido, uma vez que este processo não define um sistema de gerenciamento de qualidade, apenas garante que toda a estrutura de suporte ao serviço seja implantada da melhor maneira possível, reduzindo assim a probabiliade de *downtimes* inesperados. Todos os outros requisitos são completamente atendidos pelo processo, que é apresentado em detalhes na seção 3.4.13.

4.2.11 O Sistema de Gerenciamento do Conhecimento de Serviço e o COBIT®

Este sistema é o responsável por garantir que todas as informações importantes da TI sejam registradas e disponibilizadas, a fim de dar suporte a tomadas de decisão. Sendo assim, ele é capaz de atender aos seguintes requisitos de processos do COBIT®:

1. **PO2:** Uma arquitetura de informações da organização.
2. **PO5:** Gerenciar o investimento.
3. **AI4:** Transferir conhecimento para os gerentes do negócio, a equipe de suporte e os usuários.
4. **AI6:** Informar os gerentes do negócio sobre os resultados das mudanças.
5. **AI7:** Informar os gerentes do negócio sobre os resutados da implantações.

Todos os requisitos apresentados são completamente atendidos pelo sistema, conforme visto na seção 3.4.10. Para que fique clara a solução do requisito número dois, vale ressaltar novamente que este sistema apresenta todas as informações relevantes ao gerenciamento de serviços de TI. Sendo assim, a partir dele é possível e totalmente praticável que todos os investidores avaliem o ROI, bem como qualquer informação necessária para que se possa gerenciar os investimentos no setor.

4.3 A Operação de Serviço e o COBIT®

Esta fase do ciclo de vida do ITIL® é responsável pelo andamento das funções e processos do setor através do ciclo de vida. Os processos PO4 e DS13 do cobit estão diretamente ligados à essas atividades, uma vez que eles apresentam como principais requisitos um *framework* de processos de TI, e o gerenciamento de operações, respectivamente.

4.3.1 O Gerenciamento de Eventos e o COBIT®

Com o objetivo de avaliar a situação da infra-estrutura de TI e dos serviços, este processo monitora todos os eventos que ocorrerem dentro da TI como parte de uma operação normal, além de detectar e escalar condições de exceção. Desta forma, este processo é capaz de atender aos seguintes requisitos de processos do COBIT®:

1. **DS3:** Gerenciar a performance e a capacidade.

2. **DS8:** Gerenciar a Central de Serviços e os incidentes.

3. **DS13:** Gerenciar as operações de TI.

Uma vez que este processo apenas gera registros e alertas relativos a eventos na infra-estrutura de TI (seção 3.4.15), conclui-se que os requisitos apresentados anteriormente são parcialmente atendidos. Isto porque ele não define procedimentos para realizar os requisitos um, dois e três, apenas gera os dados necessários para essas atividades.

4.3.2 O Cumprimento de Requisição e o COBIT®

O processo de Cumprimento de Requisição gerencia as requisições comuns da operação, sejam elas de usuários ou clientes. Desta forma, este processo é capaz de atender aos seguintes requisitos de processos do COBIT®:

1. **AI6:** Gerenciar Mudanças.

2. **AI7:** Revisão pós-implementação.

Os requisitos acima são apenas atendidos, uma vez que o processo define procedimentos apenas para o estabelecimento de um canal de comunicação com os usuários e clientes, conforme foi apresentado na seção 3.4.16. Assim, através deste canal é possível avaliar o resultado de mudanças e implantações e a satisfação do cliente quanto a elas, além de ser um dos principais meios para se encontrar erros de implementação.

4.3.3 O Gerenciamento de Incidentes e o COBIT®

Este processo concentra-se em restaurar os serviços interrompidos o mais rápido possível, a fim e minimizar o impacto no negócio. Sendo assim, ele é capaz de atender aos seguintes requisitos de processos do COBIT®:

1. **DS8:** Gerenciar a Central de Seviços e os incidentes.

Considerando que para o ITIL® a Central de Serviços é uma função (seção 3.5.1) que é gerenciada pela fase de operação de serviços, o requisito apresentado é totalmente atendido pelo processo, que é detalhado na seção 3.4.14.

4.3.4 O Gerenciamento de Problemas e o COBIT®

O processo de Gerenciamento de Problemas é responsável por encontrar causas raíz de incidentes e eventos, e trabalhar pró-ativamente a fim de reduzir futuros problemas e incidentes. Desta forma, este processo é capaz de atender aos seguintes requisitos de processos do COBIT®:

1. **AI2:** Garantir a segurança e a disponibilidade das aplicações.
2. **AI4:** Transferir conhecimento para as equipes de suporte.
3. **DS10:** Gerenciar problemas.

Todos os requisitos apresentados anteriormente são completamente atendidos pelo processo, que é detalhado na seção 3.4.17. Vale ressaltar que o requisito número um é atendido pelo fato de este processo ser aplicado a qualquer tipo de problema, inclusive de segurança.

Quando se descobre um problema são realizados determinados procedimentos a fim de eliminá-lo. Estas atividades, por sua vez, disseminam conhecimento às equipes de suporte, atendendo assim o requisito número 2.

4.3.5 O Gerenciamento de Acesso e o COBIT®

Este processo deve cuidar para que apenas usuários autorizados tenham acesso aos sistemas da organização. Assim sendo, este proceso é capaz de atender ao seguinte requisito de processo do COBIT®:

1. **DS5:** Gerenciamento de contas de usuário.

O requisito apresentado acima é totalmente atendido pelo processo, que é detalhado na seção 3.4.18.

4.4 A Melhoria de Serviço Continuada e o COBIT®

A fase de Melhoria de Serviço Continuada do ITIL® deve desempenhar atividades visando melhorar a eficiência, maximizar a efetividade e otimizar os custos inerentes aos serviços de TI. O PO8 é o processo do COBIT® diretamente ligado a esta fase, uma vez que um dos seus principais requisitos é obter a melhoria contínua de TI.

4.4.1 O Processo de Melhoria dos Sete Passos e o COBIT®

Este processo fundamenta-se no conceito de que a CSI é fundamentada em medições, objetivando reduzir as lacunas constantemente encontradas entre os objetivos de negócio e de TI. Desta forma, este processo é capaz de atender os seguintes requisitos de processos do COBIT®:

1. **PO8:** Implementar melhoria contínua.
2. **ME1:** Monitorar e avaliar a performance de TI.
3. **ME2:** Monitorar e avaliar o controle interno.
4. **ME3:** Assegurar a conformidade com os requisitos externos.

Todos os requisitos apresentados anteriormente são atendidos pelo processo, que é detalhado na seção 3.4.19.

Os processos ou requisitos do COBIT® que não foram discriminados neste capítulo não estão relacionados ao Gerenciamento de Serviços, e desta forma, devem ser alinhados aos *frameworks* das outras áreas de governança. A seguir, é apresentada uma tabela contendo todos os relacionamentos apresentados até o momento, objetivando proporcionar uma visão mais prática do alinhamento realizado. O campo de relacionamento encontrado nos processos do ITIL define, como segue:

- A: Atende ao requisito do processo apresentado.
- AP: Atende Parcialmente ao requisito do processo apresentado.
- I: Influencia o requisito do processo apresentado.

Tabela 4.1: Alinhamento entre os *frameworks* ITIL® e COBIT®.

ITIL®		**COBIT®**	
Processo	Relac.	Processo	Requisito
Gerenciamento Financeiro	A	PO1	O Gerenciamento do Valor de TI;
	A	PO5	Um *Framework* de Gerenciamento Financeiro;
	A	DS6	A contabilização e a modelagem de custo.

Gerenciamento da Demanda	AP	PO1	O Plano Estratégico de TI;
	AP	PO8	O Foco no Cliente através do Gerenciamento da Qualidade;
	I	DS1	A definição dos Níveis de Serviço.
Gerenciamento do Portfólio de Serviço	A	PO1	O Gerenciamento de Portfólio;
	A	PO4	Priorizar os recursos, de acordo com a necessidade;
	A	PO5	O Gerenciamento de Investimento.
	I	DS1	Definir e Gerenciar Níveis de Serviço;
	A	DS6	A definição dos serviços com relação aos custos.
Gerenciamento do Catálogo de Serviço	A	PO4	Um *framework* de processos de TI que garanta transparência e controle;
	A	DS1	A definição dos serviços.
Gerenciamento de Nível de Serviço	A	PO4	Definir os relacionamentos entre o setor de negócios e o de TI;
	AP	PO8	Obter melhoria contínua de processos;
	A	AI5	Gerenciar os contratos com fornecedores;
	A	DS1	Gerenciar os níveis de serviço;
	A	DS2	Gerenciar serviços de terceiros;
	A	ME1	Obter dados através de monitoramento, e avaliar a performance.
Gerenciamento da Capacidade	A	PO3	Definir uma direção tecnológica para suportar o negócio;
	A	AI1	Definir e manter os requisitos funcionais de negócio;
	A	DS3	Gerenciar a performance e a capacidade;
	A	DS13	Reduzir os atrasos de negócio e os custos de operações de TI.
Gerenciamento da Disponibilidade	A	DS3	Manter a disponibilidade dos recursos;

	A	DS4	Garantir continuidade, sustentabilidade e a confiabilidade dos serviços.
Gerenciamento da Segurança da Informação	A	AI3	Proteção e disponibilização dos recursos de infra-estrutura;
	A	DS5	Gerenciar a segurança de TI e definir um programa de segurança;
Gerenciamento de Fornecedores	A	AI5	Gerenciar contratos com fornecedores;
	A	DS2	Monitorar a performance dos fornecedores.
Gerenciamento da Continuidade do Serviço de TI	A	PO9	Estabelecer um *framerowk* para o gerenciamento de riscos;
	A	AI1	Apresentar um relatório de análise de riscos;
	A	DS4	Gerenciar a Continuidade dos serviços.
Gerenciamento da Mudança	A	AI6	Gerenciar Mudanças.
Gerenciamento da Configuração e de Ativo de Serviço	A	DS9	Gerenciar a Configuração.
Gerenciamento de Liberação e Implantação	AP	PO8	Um Sistema de Gerenciamento de Qualidade;
	A	AI3	Um ambiente de teste de viabilidade;
	A	AI4	Disseminar todas as formas de conhecimento com relação a novos sistemas;
	A	AI7	Instalar e credenciar soluções, oferecer um ambiente de teste e realizar revisões de pós-implementação.
Sistema de Gerenciamento do Conhecimento de Serviço	A	PO2	Uma arquitetura de informações da organização;
	A	PO5	Gerenciar o investimento;
	A	AI4	Transferir o conhecimento para os gerentes do negócio, a equipe de suporte e os usuários;

	A	AI6	Informar os gerentes do negócio sobre os resultados das mudanças;
	A	AI7	Informar os gerentes do negócio sobre os resultados das implantações.
Gerenciamento de Eventos	AP	DS3	Gerenciar a performance e a capacidade;
	AP	DS8	Gerenciar a Central de Serviços e os incidentes;
	AP	DS13	Gerenciar as operações de TI.
Cumprimento de Requisição	A	AI6	Gerenciar Mudanças;
	A	AI7	Revisão de pós-implementação.
Gerenciamento de Incidentes	A	DS8	Gerenciar a Central de Serviços e os incidentes.
Gerenciamento de Problemas	A	AI2	Garantir a segurança e a disponibilidade das aplicações;
	A	AI4	Transferir conhecimento para as equipes de suporte;
Gerenciamento de Problemas (*cont.*)	A	DS10	Gerenciar Problemas.
Gerenciamento de Acesso	A	DS5	Gerenciamento de Contas de Usuário.
Processo de Melhoria dos Sete Passos	A	PO8	Implementar melhoria contínua;
	A	ME1	Monitorar e avaliar a performance de TI;
	A	ME2	Monitorar e avaliar o controle interno;
	A	ME3	Assegurar a conformidade com os requisitos externos;

Conclusão

Devido à importância da informação como recurso estratégico, a aplicação de TIC tornou-se um ponto central na estratégia e nos processos de negócio de várias organizações. Desta forma, para obter sucesso essas organizações precisam adquirir conhecimento sobre os riscos e restrições de TIC em todos os níveis dentro da empresa, objetivando um controle efetivo desses recursos. Para tais necessidades, o COBIT® apresenta-se como o *framework* de controle e segurança de TIC mundialmente mais aceito, sendo capaz de habilitar a Governança de TIC para a organização e, assim, fazer com que esta faça uso de suas informações de maneira ótima, com melhoria contínua de processos, redução de custos e alinhamento das funções de TIC às necessidades do negócio.

Neste mesmo cenário, a prestação de serviços surge como uma atividade de extrema importância econômica, devido à sua popularidade no âmbito de TIC. Atualmente, muitas empresas terceirizam soluções extremamente importantes que, direta ou indiretamente, influenciam fortemente os resultados dos seus negócios. Devido à intangibilidade do valor dos serviços prestados e à grande concorrência do setor, os fornecedores desses serviços devem aplicar esforços consideráveis a fim de garantir utilidade e garantia às soluções que entregam aos clientes. Para atender a essas e outras necessidades, a biblioteca ITIL® define um ciclo de vida de serviços, bem como um conjunto de processos a fim de garantir o valor dos serviços prestados.

A fim de atender as necessidades apresentadas, foi desenvolvida neste trabalho uma abordagem para o alinhamento entre esses dois *frameworks*, referenciando cada processo do ITIL® aos requisitos do COBIT® que por eles fossem atendidos ou influenciados. Dos trinta e quatro processos do COBIT®, vinte e seis apresentam pelo menos um requisito relacionado ao Gerenciamento de Serviços de TIC. O COBIT®, que pode ser utilizado no mais alto nível de Governança de TIC, define vários requisitos quanto ao Gerenciamento de Serviços que, por sua vez, são completamente atendidos pelo ITIL® (seção 4).

A adoção de padrões e melhores práticas permite uma rápida implementação de bons procedimentos, evitando assim os atrasos causados pela criação de novas abordagens para tratar assuntos conhecidos, prática que é classificada por muitos profissionais da área como "reinventar a roda". Por fim, a abordagem apresentada neste trabalho deve ser de grande valia às organizações prestadoras de serviço de TIC, uma vez que elas precisam gerenciar suas informações e, ao mesmo tempo, fazer com que o cliente perceba valor nos serviços por elas

prestados.

Referências Bibliográficas

[1] Alan Calder. *Implementing Information Security based on ISO 27001/ISO 27002*. Van Haren Publishing, 2009.

[2] Christopher Fox and Paul Zonneveld. *IT Control Objectives for Sarbanes-Oxley*, volume 2. IT Governance Institute, 2006.

[3] Erik Guldentops, Roger Debreceny, Steven de Haes, Roger Lux, John Mitchell, Ed O'Donnel, Scott Summers, and Wim Van Grembergen. *Cobit Students Book*. IT Governance Institute, 2004.

[4] IT Governance Institute. *COBIT 4.1*. ITGI, 2007.

[5] Ralf Kneuper. *CMMI: Improving Software and Systems Development Process Using Capability Maturity Model Integration (CMMI-DEV)*. Roocky Nook, 2009.

[6] Kloesteboer L. Implementing itil v3 configuration management. IBM Press, 2008.

[7] Paul R. Niven. *Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results*. Wiley, 2006.

[8] Alex D. Paul. *Itil Heroes' Handbook: Itil For Those Who Don'T Have The Time*. CreateSpace, Paramount, CA, 2009.

[9] Thomas Pyzdek and Paul Keller. *The Six Sigma Handbook*. McGraw-Hill Professional, 2009.

[10] Cynthia Snyder Stackpole. *A Project Manager's Book of Forms: A Companion to the PMBOK Guide*. Wiley, 2009.

[11] Sharon Taylor, David Cannon, and David Wheeldon. *ITIL Version 3 - Service Operation*, volume 4. OGC - Office of Government Commerce, 2007.

[12] Sharon Taylor, Gary Case, and George Spalding. *ITIL Version 3 - Service Improvement*, volume 5. OGC - Office of Government Commerce, 2007.

[13] Sharon Taylor, Majid Iqbal, and Michael Nieves. *ITIL Version 3 - Service Strategy*, volume 1. OGC - Office of Government Commerce, 2007.

[14] Sharon Taylor, Shirley Lacy, and Ivor MacFarlane. *ITIL Version 3 - Service Transition*, volume 3. OGC - Office of Government Commerce, 2007.

[15] Sharon Taylor, Vernon Lloyd, and Colin Rudd. *ITIL Version 3 - Service Design*, volume 2. OGC - Office of Government Commerce, 2007.

[16] Masashi Une and Masashi Une. The security evaluation of time stamping schemes: The present situation and studies. In *IMES Discussion Papers Series 2001-E-18*, pages 100–8630, 2001.

[17] Bom J V. Foundations of it service management base on itil v3. Van Haren Publishing for itSMF, 2006.

[18] Peter Weil and Jeanne W. Ross. *IT Governance - How Top Performers Manage IT Decision Rights for Superior Results*, volume 1. Harvard Business Press, 2004.

[19] P. Williams. *Optimizing Returns From IT-related Business Investments*, volume 5. ISACA, 2005.

[20] Álvares E., Giacometti C., and Gusso E. *Governança Corporativa: Um modelo brasileiro.* Elsevier, 2008.