



Faculdade Lourenço Filho
Ciência da Computação

COBIT, ITIL e ISO/IEC 27002 Melhores Práticas para Governança de Tecnologia da Informação

por

Alexandre Cavalcante Alencar

Orientador:
José Alzir Bruno Falcão

Fortaleza, 2010

COBIT, ITIL e ISO/IEC 27002 Melhores Práticas para Governança de Tecnologia da Informação

Alexandre Cavalcante Alencar

Monografia apresentada ao curso de
Ciência da Computação da Faculdade
Lourenço Filho como requisito parcial
para obtenção do título de Bacharel em
Ciência da Computação.

Orientador:
José Alzir Bruno Falcão

Março, 2010

COBIT, ITIL e ISO/IEC 27002 Melhores Práticas para Governança de Tecnologia da Informação

Alexandre Cavalcante Alencar

Monografia Apresentada ao curso de Bacharel em Ciências da Computação da Faculdade Lourenço Filho, como parte dos requisitos para a obtenção do grau de Bacharel em Ciências da Computação.

Composição da Banca Examinadora:

Prof. MSc. José Alzir Bruno Falcão (Orientador)

Prof. Msc. Carlos Alberto Manso

Prof. MSc. William de Araujo Sales

Aprovada em 04 de Março de 2010

A Lídia Cavalcante Alencar
In memoriam Antonio Alencar

Agradecimentos

A Tatiane Ramos, minha companheira durante esta longa jornada, que dedicou seu apoio incondicional, mesmo com todos os sacrifícios que se fizeram necessários ao longo dos últimos anos.

Aos amigos(as), professor(as), funcionários(as) que fizeram parte deste capítulo que compõe a história da minha vida.

“A luta contra o erro tipográfico tem algo de homérico. Durante a revisão os erros se escondem, fazem-se positivamente invisíveis. Mas assim que o livro sai, tornam-se visibilíssimos...”

(Monteiro Lobato)

Resumo

Hoje, os departamentos de TI das organizações têm a necessidade de uma abordagem de melhores práticas, que são muito parecidas e oferecem soluções semelhantes para os vários problemas de uma organização, mas em muitos casos, não está claro como seguir ou aplicar cada uma delas em conjunto com outras ferramentas, tornando a utilização destas melhores práticas complexa.

A intenção com este trabalho é fornecer uma visão geral das melhores práticas existentes, embora reconheça que algumas das melhores práticas são adequadas para uma organização, ao mesmo tempo que para outras podem não ser apropriadas. Em conclusão, quanto mais conhecemos sobre as melhores práticas, ignoramos o potencial da utilização e aplicação destas nas organizações em prejuízo para o negócio.

Um aspecto importante a considerar, antes de partir para a explicação das melhores práticas, é ter conhecimento sobre o funcionamento da empresa onde se pretende utilizá-las, de forma que se possa gerar oportunidades de melhoria, resultando em ganhos reais para o negócio.

Palavras-chave: ITIL, COBIT, ISO/IEC 27001:2005, ISO/IEC 27002:2005, Governança, Tecnologia da Informação, Segurança da Informação, Gerenciamento de Serviços

Abstract

Today, organizations IT departments have a need for a best practice approach, which are very similar and offer similar solutions to the various problems of an organization, but in many cases, it is unclear how to follow or apply each one with other tools, making use of best practice complex.

The goal of this work is to provide an overview of best practices, while recognizing that some of them are appropriate for an organization, while for others may not be. In conclusion, more we know about best practices, more we ignore the potential use and application of these to organizations, resulting in damage to the business.

An important aspect to consider before leaving for the explanation of best practice, it is essential to have excellent knowledge of the business of the company where you want to use them, so that it can generate opportunities for improvement, resulting in real gains for the business.

Keywords: ITIL, COBIT, ISO/IEC 27001:2005, ISO/IEC 27002:2005, Governance Information Technology, Information Security, Service Management

Sumário

Introdução.....	1
Capítulo 1 - O Gerenciamento de Serviços, a Segurança da Informação e a Governança de TI.....	3
1.1. Gerenciamento de Serviços de TI.....	3
1.2. A Segurança da Informação.....	3
1.2.1. Engenharia da Segurança	4
1.2.2. Proteção da privacidade.....	5
1.2.3. Tolerância a Invasões.....	5
1.2.4. Detecção de Intrusões.....	6
1.3. A Governança de TI.....	6
1.4. Metodologias.....	9
Capítulo 2 - A metodologia ITIL.....	10
2.1. Estratégia de Serviços.....	12
2.2. Desenho de Serviços.....	13
2.3. Transição de Serviços.....	13
2.4. Operação de Serviços.....	14
2.5. Melhoria Continuada de Serviços.....	14
Capítulo 3 – A Metodologia ISO/IEC 27002.....	17
Capítulo 4 – A Metodologia COBIT.....	22
Conclusão.....	29
Bibliografia.....	31
ANEXO I - Mapeamento de Metas de Negócios em Metas de TI.....	33
ANEXO II - Mapeamento de Metas de TI em Processos de TI.....	34
ANEXO II - Mapeamento de Metas de TI em Processos de TI.....	35
ANEXO III – Descrições dos Processos do COBIT 4.1.....	36
ANEXO IV – Plano de Ações para Implementação da Governança de TI.....	71
ANEXO V – Relação entre processos dos frameworks COBIT e ITIL.....	73
ANEXO VI – Relação entre processos dos frameworks ISO/IEC 27002 e ITIL.....	75

Lista de Figuras

Figura 1: O ciclo de melhoria continuada do ITIL, adaptado de OGCe, 2007, p.33.....	10
Figura 2: Ciclo de Vida do ITIL v3, Fonte OGCf, 2007.....	12
Figura 3: O processo de melhoria em 7 passos, adaptado de OGCe, 2007.....	15
Figura 4: Modelo PCDA como usado em SGSI, Fonte ISO/IEC 27002.....	18
Figura 5: Os domínios do COBIT, adaptado de ITGIb, 2007, p.27.....	24
Figura 6: O modelo de governança COBIT, adaptado de ITGIb, 2007, p.28.....	25
Figura 7: COBIT e outros padrões, do autor.....	28

Lista de Tabelas

Tabela 1: Áreas de Foco da Governança de TI, adaptado de ITGlb, 2007, p.06.....	7
Tabela 2: Processos e Funções do ITIL v3, adaptado de OGCf, 2007.....	11
Tabela 3: Como a governança e os negócios dirigem a TI, adaptado de ITGlb, 2007....	22
Tabela 4: Mapeamento de metas de negócios em metas de TI, adaptado de ITGlb, 2007	33
Tabela 5: Mapeamento de metas de TI em processos de TI, adaptado de ITGlb, 2007..	34
Tabela 6: Relação entre processos dos frameworks COBIT e ITIL, do autor.....	73
Tabela 7: Relação entre processos dos frameworks ISO/IEC 27002 e ITIL, do autor....	75

Introdução

É possível afirmar que os serviços prestados pela área de TI (Tecnologia da Informação) das organizações é cada vez mais importante para a execução das atividades diárias de negócio, garantindo assim maior competitividade no mercado, através do ganho de produtividade gerado pelas ferramentas tecnológicas a disposição da organização.

Atualmente, os sistemas e os serviços de TI desempenham um papel vital na coleta, análise, produção e distribuição da informação indispensável à execução do negócio das organizações. Dessa forma, tornou-se essencial o reconhecimento de que a TI é estratégica e um importante recurso que precisa de gestão e investimentos apropriados. Esse cenário motivou o surgimento do conceito de Governança de TI, do termo em inglês *IT Governance*, através da qual se procura o alinhamento da TI com os objetivos da organização. A Governança de TI define a TI como um fator essencial para a gestão financeira e estratégica de uma organização e não apenas um suporte às mesmas (BERNARDES e MOREIRA, 2007, p. 01).

Com a dependência da área de negócio das empresas nos serviços oferecidos pela TI, é de extrema importância que seja possível gerenciá-los de forma a permitir que as pessoas de negócio se concentrem em suas atividades e que marcos regulatórios possam ser atendidos pela organização. Desta forma, as melhores práticas de gestão de serviços, segurança, projetos, riscos e governança desempenham papel fundamental no alinhamento das estratégias de negócio da organização com o funcionamento da TI, proporcionando assim o uso eficiente e eficaz dos recursos de TI da organização.

Segundo (WEILL e ROSS, 2006, p. 02), extrair maior valor da TI para a organização não é uma questão de se trabalhar com mais afinho ou por mais tempo. Na verdade, é uma questão de se requerer um envolvimento de pessoas de diferentes áreas nas decisões de TI, bem como, de uma concepção de novas maneiras de se tomar decisões ou de desenvolvimento de novas técnicas para implementar tais decisões.

A utilização de boas práticas para Gestão de Serviços e Governança de TI nas pequenas e médias empresas cearenses é precária por falta de capacitação dos gestores e funcionários, da ausência de investimentos e do desconhecimento da importância e dos riscos inerentes a uma gestão incorreta dos recursos de TI de uma organização.

Com a crescente demanda por serviços de TI nas áreas de negócios das organizações, se faz necessário uma gestão transparente e que agregue valor através da entrega de serviços com qualidade e garantia.

Segundo (Becker et al., 2007), poucas são as empresas que se adequam plenamente aos princípios de governança de TI. Em pesquisa realizada pela Modulo Security com as empresas que possuem ações na Bolsa de Valores de São Paulo, apenas 25% destas possuem projetos formais de governança de TI (MODULO, 2006). Para as que buscam adequar-se, em detrimento das resistências internas, comuns em qualquer processo que envolve transparência, por insegurança ou até mesmo por completo desconhecimento do assunto, falta o entendimento dos benefícios que a governança de TI pode prover, bem como por onde começar.

Por ser um tema recente, e com a quantidade limitada de pesquisas e publicações acadêmicas que possam servir de referência para administradores interessados no assunto, o desenvolvimento deste trabalho, com uma síntese das principais referências técnicas e com uma visão geral dos *frameworks* de governança de TI, tem o seu valor para a comunidade acadêmica e profissionais da área.

O objetivo deste trabalho é apresentar os principais *frameworks* para Gestão de Serviços, com o ITIL (*Information Technology Infrastructure Library*), Gestão de Segurança da Informação, com a ISO/IEC 27002 e Governança de TI com o COBIT (*Control Objectives for Information and Related Technology*), suas práticas e processos para a gestão, auditoria e controle do ciclo de vida dos Serviços de TI.

Este trabalho está organizado em quatro capítulos. No primeiro capítulo é apresentada uma introdução ao gerenciamento de serviços de TI, segurança da informação e governança de TI. No segundo, terceiro e quarto capítulos são apresentados os *frameworks* de melhores práticas ITIL, ISO/IEC 27002 e COBIT respectivamente, seus princípios e práticas. Encerramos com as conclusões que incluem nossas considerações sobre a pesquisa realizada, o trabalho desenvolvido e os futuros trabalhos a serem realizados.

Capítulo 1 - O Gerenciamento de Serviços, a Segurança da Informação e a Governança de TI

1.1. Gerenciamento de Serviços de TI

Para que seja possível entender o que é Gerenciamento de Serviços, se faz necessário o entendimento do conceito de serviço e como o seu gerenciamento pode auxiliar aos provedores de serviços a entregarem a proposição de valor de TI ao negócio. A gestão de serviços tem origem em negócios tradicionais como linhas aéreas, bancos, hotéis, companhias telefônicas e energéticas (OGCf, 2007, p.5).

Segundo (OGCf, 2007, p.5) “Um serviço é um meio de proporcionar valor aos clientes, possibilitando-lhes alcançar resultados desejados evitando custos e riscos específicos”. Como o conceito de serviço pode ser utilizado nos mais diversos contextos, é assumido aqui como um meio de entregar valor, e este conceito deve estar na essência da definição de serviços por uma organização.

De forma simplificada, o Gerenciamento de Serviços de TI (GSTI) é um grupo de processos e funções que lubrificam as engrenagens da máquina da TI. Sem o GSTI, os projetos e sistemas de TI poderão deteriorar-se ao longo do tempo até que estes falhem.

De acordo com (OGCf, 2007, p.5), o GSTI está empenhado a entregar e suportar serviços de TI apropriados para as necessidades do negócio de uma organização. O ITIL (OGCf, 2007, p.6) provê um conjunto compreensivo, consistente e coerente de processos das melhores práticas para GSTI, proporcionando ao negócio o uso eficiente e eficaz dos sistemas de informação.

1.2. A Segurança da Informação

A segurança da informação é uma das pedras angulares da Sociedade da Informação. Integridade das transações financeiras, prestação de contas para assinaturas eletrônicas, a confidencialidade dentro de uma empresa virtual, privacidade da informação pessoal, dependência em infra-estrutura crítica, tudo depende da disponibilidade de mecanismos de segurança fortes e confiáveis. Garantir a disponibilidade desses mecanismos requer a solução de vários problemas substanciais de pesquisa e desenvolvimento.

Segundo (NIST, 2006, p. 02), a governança da segurança da informação pode ser definida como o processo de estabelecer e manter um *framework* de apoio e estrutura de gestão e processos para garantir que as estratégias de segurança da informação estão alinhados com objetivos de negócio e de apoio, são consistentes com as leis e regulamentos aplicáveis mediante a adesão às políticas e controles internos e fornecer a atribuição de responsabilidade, tudo em um esforço de gestão de risco.

As empresas dependem fortemente de tecnologia da informação para executar suas operações diárias e oferecer produtos e serviços. Com uma dependência e complexidade crescente em TI e sua infra-estrutura, a segurança da informação tornou-se uma função essencial por conta das ameaças em constante mutação. Esta função deve ser gerida e regulada para reduzir os riscos de operações das empresas e garantir a capacidade destas realizarem seus negócios e servir aos seus clientes.

O objetivo da governança da segurança da informação é assegurar que as empresas estão ativamente implementando controles adequados para suportar seus negócios em uma relação custo-eficácia, enquanto gerenciam a evolução de riscos. Como tal, a governança da segurança da informação tem seu próprio conjunto de necessidades, desafios, atividades e tipos de estruturas possíveis, além de uma função decisiva na identificação dos principais papéis e responsabilidades, que influencia no desenvolvimento de políticas, supervisão e acompanhamento de atividades em curso.

1.2.1. Engenharia da Segurança

A construção de sistemas seguros precisa evoluir de uma arte para uma disciplina de Engenharia de Segurança, com métodos bem definidos para a construção desde seus componentes básicos até a avaliação e validação formal da segurança. Noções de composição da segurança precisam ser desenvolvidas, combinando técnicas de engenharia de software, projeto de hardware seguro, métodos formais e criptografia. Embora a comunidade científica tenha feito muitos progressos nesta direção, mas não obstante, a Engenharia da Segurança está mais perto do empirismo do que para a ciência: o número de novas vulnerabilidades ainda cresce a uma taxa assustadora (ISO/IEC 27002, 2005, p.5).

1.2.2. Proteção da privacidade

A medida que o uso de serviços eletrônicos aumenta, a tecnologia que permite às empresas coletar, armazenar, analisar e transferir informações sobre seus usuários evolui (FTC, 2000). Diante disto, as questões sobre a privacidade despertam a preocupação de autoridades, empresas e usuários que precisam garantir que regulamentações legais sejam obedecidas e tais informações não sofram acesso por pessoas não autorizadas. A proteção da privacidade na sociedade da informação vai além de uma política de segurança da informação (RFC2196, 1997). É preciso também atentar a três aspectos principais:

- I. Ferramentas que permitam a usuários comuns, sem conhecimento técnico, controlarem as informações reveladas sobre si;
- II. Modelos de negócios e processos que equilibrem a informação pessoal que consomem e o valor que geram para o cliente;
- III. Ferramentas que permitam às empresas definir e fazer cumprir suas práticas de privacidade, e para gerir a identidade e a informações do perfil que lhe são transmitidas de uma forma confiável e responsável.

Para que seja possível atender a todos os aspectos necessários a um bom funcionamento de políticas de privacidade, o desenvolvimento de tecnologias para a gestão da privacidade acabam se tornando um elemento comum na construção de novos produtos e serviços da empresa.

1.2.3. Tolerância a Invasões

Uma dos tópicos de pesquisa e desenvolvimento mais importantes é o desenvolvimento de sistemas de tolerância a invasões: tais sistemas funcionam de forma segura e confiável, mesmo que alguns subsistemas sejam atacados e maliciosamente corrompidos - o que é inevitavelmente, o caso da maioria das grandes aplicações (PARTHA et al., 2000). Estes podem até mesmo reagir a intrusões detectadas, reconfigurando-se em um estado menos corrompido. Ao longo dos últimos anos, muito trabalho foi feito no desenvolvimento de mecanismos de tolerância a intrusão, em particular no contexto de comunicação em grupo e replicação de serviços. Mais trabalhos serão necessários no que diz respeito a sistemas tolerantes a invasões, principalmente em relação aos baseados em grandes grupos dinâmicos e provisórios (*ad-hoc*). Para novos sistemas confiáveis, meios de tolerância a intrusões, autenticação, autorização e gestão precisam ser desenvolvidos.

1.2.4. Detecção de Intrusões

Um tema muito relacionado é o de detecção de intrusão: Como detectar intrusões, ou, mais geralmente, situações de alto risco? Muitos sensores foram desenvolvidos para observar estas situações específicas, e as ferramentas para correlacionar alarmes gerados por sensores diferentes, de modo a obter uma melhor visão. Mas ainda os principais problemas continuam em aberto: os sistemas de detecção de intrusão geram, de longe, muitos alarmes falsos, e raramente sugerem reações eficazes em alarmes verdadeiros. Mais pesquisa e desenvolvimento são necessários para que haja uma melhora significativa na qualidade e significado dos alarmes, por exemplo, considerando semanticamente mais camadas e aplicações específicas (PTACEK e NEWSHAM, 1998).

1.3. A Governança de TI

As necessidades de governança de TI originaram-se das demandas de controle, transparência e previsibilidade das organizações. As origens destas demandas datam do começo dos anos 90, quando as questões relativas à qualidade ganharam uma enorme importância no cenário mundial. O crescimento exuberante da economia mundial prevaleceu apesar da forte demanda por melhores mecanismos de controle e acompanhamento de resultados, por consequência, o processo de maturidade da governança nas empresas acabou sendo adiado por alguns anos. (MANSUR, 2007, p. 5).

Para que se possa atingir o mínimo de Governança, cinco áreas inter-relacionadas da TI precisam de atenção, para que a organização obtenha êxito nos seus processos e otimização nos seus investimentos em TI: (1) os processos de TI; (2) a arquitetura de TI; (3) a infra-estrutura de TI; (4) as necessidades de aplicações do negócio e (5) os investimentos e a priorização de TI. (WEILL e ROSS, 2006, p. 27-28).

Segundo (ISACA, 2007, p.14), a governança de TI é definida como uma estrutura de relacionamentos e processos para direcionar e controlar o processo de alcançar os objetivos de negócio, adicionando valor e balanceando riscos sobre os investimentos em TI e seus processos.

A governança de TI é de responsabilidade dos executivos e conselho diretor, e consiste da liderança, estruturas organizacionais e processos para garantir que as iniciativas de TI da organização sustentam e estendem as estratégias e objetivos de negócio, através do balanceamento entre os objetivos de conformidade e desempenho, conduzido pelos executivos.

Segundo (ITGIb, 2007. p.06), a governança de TI tem como foco o alinhamento estratégico, entrega de valor, gerenciamento de recursos, gerenciamento de riscos e medição do desempenho. Buscando com isso a conexão entre os planos da TI e do negócio, suportando a proposição de valor e o alinhamento com as estratégias do negócio e as operações de TI. Assim, a governança de TI garante que há objetivos acordados para a TI, gerenciamento e controle em atuação, bem como a medição de desempenho de forma a evitar retornos inesperados. Na Tabela 1 são apresentadas as áreas de foco da Governança de TI segundo (ITGIb, 2007, p.06).

Área de Foco	Descrição
Alinhamento estratégico	Concentra-se em assegurar a articulação de negócios e planos de TI, sobre a definição, manutenção e validação da proposta de valor de TI, e alinhar as operações de TI com as operações de negócios.
Entrega de valor	Concentra-se em como executar a proposição de valor ao longo do ciclo de entrega, garantindo que ele proporciona os benefícios prometidos contra a estratégia; Concentrar na otimização de custos e proporcionando o valor intrínseco de TI.
Gerenciamento de recursos	Concentra-se na otimização do investimento e a gestão adequada dos recursos críticos de TI, tais como aplicações, informações, infra-estrutura e pessoas. Questões fundamentais relacionadas com a otimização de conhecimentos e de infra-estrutura.
Gerenciamento de risco	Requer a consciência de risco por altos funcionários das empresas, uma compreensão clara do apetite da empresa para o risco, uma compreensão dos requisitos de conformidade, transparência sobre riscos significativos para a empresa, e a incorporação das responsabilidades de gestão de risco na organização.
Medição de desempenho	Acompanha e monitora a implementação da estratégia, a conclusão do projeto, o uso de recursos, o desempenho do processo e prestação de serviços, utilizando, por exemplo, <i>balanced scorecards</i> que traduzir a estratégia em ação para objetivos mensuráveis, muito além de resultados contábeis convencionais.

Tabela 1: Áreas de Foco da Governança de TI, adaptado de ITGIb, 2007, p.06

A governança de TI apresenta inúmeros benefícios para as organizações, dos quais merecem destaque especial:

- **Confiança da Administração Superior:** Uma abordagem de governança de TI eficaz pode trazer todos ao mesmo lado, fornecendo uma linguagem comum, criando mecanismos claros para a tomada de decisões, e facilitar a transparência e a precisão das informações de gestão. Quando a gestão de negócio tem uma visão mais clara de como funciona a TI, sua confiança

nas decisões de investimentos aumenta.

- **Capacidade de Resposta da TI para o Negócio:** TI mais sensível às necessidades do negócio. Agilidade, flexibilidade e capacidade de resposta são atributos essenciais da função de TI em seu apoio à evolução das necessidades de negócios. A governança de TI eficaz garante cadeias de comando claras, tomada de decisão eficaz e uma maior confiança na tomada de riscos e realização de investimentos.
- **Maior Retorno sobre Investimentos (ROI):** Em média, uma alta proporção de gastos TI é perdido por meio de falhas de projeto, Infra-estrutura ineficaz e ineficiente, e processos fora do padrão e mal geridos. A governança de TI eficaz ajuda a reduzir as falhas de projeto, otimizar a infraestrutura de TI e aumentar a eficiência dos processos de TI. O maior ROI implica em maior valor ao negócio e melhor qualidade dos serviços, permitindo alcançar os objetivos de negócio.
- **Serviços mais Confiáveis:** A governança de TI garante que os processos e serviços críticos de TI são monitorados e quaisquer incidentes ou falhas de alta prioridade são abordadas e resolvidas. Serviços que requerem altos níveis de confiabilidade são implementados com uma infraestrutura robusta e resiliente, de forma a minimizar a probabilidade de falha ou interrupção do serviço. A governança de TI também garante riscos mais baixos, melhor qualidade dos serviços e maior satisfação do cliente.
- **Mais Transparência:** A boa governança ajuda fornecer a gerência informações claras, confiáveis e precisas sobre TI, tais como o status dos projetos e os custos de serviços de TI. Maior transparência significa que os interessados irão receber informações de uma forma que eles compreendam e com a confiança de que a informação possa ser utilizada. A implementação de uma estrutura eficaz de governança de TI garante que a informação certa esteja disponível para o nível certo de tomadores de decisão, caso contrário, a informação tende a ser perdida na selva de dados.

1.4. Metodologias

Existem diversos *frameworks* que visam auxiliar na Gestão de Serviços e Governança de TI, dentre os quais destaco o ITIL para Gestão de Serviços, COBIT para Auditoria e Controle e ISO 27002 para Gestão de Segurança da Informação.

A utilização destes *frameworks* em conjunto norteiam os responsáveis pelo processo de governança na implementação das melhores práticas difundidas internacionalmente, de forma que os objetivos organizacionais possam ser atendidos.

Capítulo 2 - A metodologia ITIL

No capítulo anterior, uma breve introdução ao Gerenciamento de Serviços, Segurança da Informação e Governança de TI foi apresentada, bem como sua importância para as organizações. Neste capítulo, discutiremos a metodologia ITIL, que é reconhecida mundialmente como o padrão internacional de melhores práticas para GSTI (OGCf, 2007, p.1).

Segundo (OGCf, 2007, p.2), o ITIL é um conjunto consistente de melhores práticas com vasta documentação, usadas por milhares de organizações no mundo. Consistindo de uma série de livros que dão suporte a prestação de serviços de qualidade, utilizando os recursos disponíveis para facilitar o atendimento das necessidades do negócio. O diagrama apresentado na Figura 1, é uma representação do processo de melhoria continuada do ITIL:

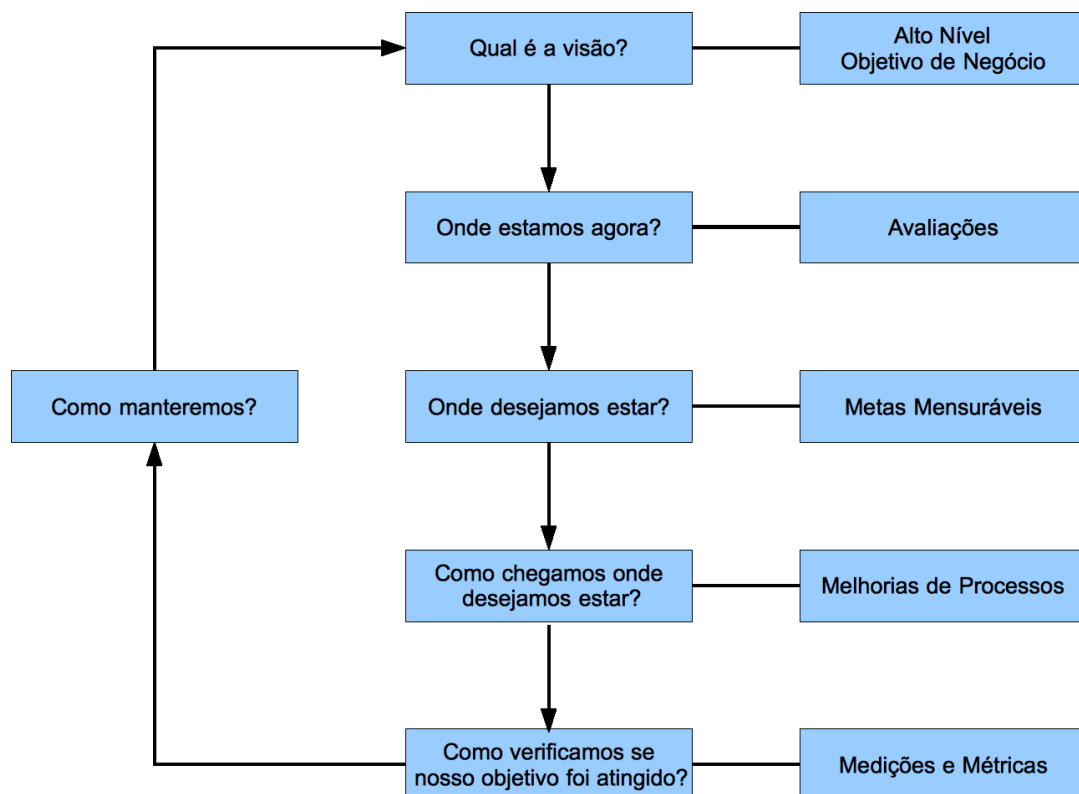


Figura 1: O ciclo de melhoria continuada do ITIL, adaptado de OGCE, 2007, p.33

A Figura 1 ilustra um ciclo constante de melhoria, bem como as muitas oportunidades para a melhoria continuada de serviços. O processo de melhoria pode ser resumido em seis etapas:

1. Compreender a visão através de objetivos de negócio de alto nível. A visão deve alinhar os negócios e estratégias de TI.

2. Avaliar a situação atual para obter uma visão exata e imparcial de onde a organização está agora. Esta avaliação inicial é uma análise da situação atual em termos de negócio, organização, pessoas, processos e tecnologia.
3. Compreender e acordar as prioridades para melhoria baseada em um profundo desenvolvimento dos princípios definidos na visão. A visão pode estar distante, mas esta etapa prevê metas específicas e uma agenda gerenciável.
4. Detalhar o plano de melhoria continuada para conseguir maior qualidade de serviços providos através da implementação de processos de GSTI.
5. Verificar se as medições e métricas estão em funcionamento para assegurar que as metas foram alcançadas, a conformidade dos processos de cumprida, e os objetivos e as prioridades de negócios foram atendidas pelo nível de serviço.
6. Finalmente, o processo deve assegurar que o ritmo de melhoria da qualidade é mantida, assegurando que as mudanças sejam incorporadas na organização.

O *framework* ITIL v3 é composto por cinco estágios, que por sua vez possuem processos conforme ilustrado na Tabela 2. Um sumário dos estágios é apresentado no texto que se segue.

Publicações	Processos	Funções
Estratégia de Serviço	- Gerenciamento Financeiro de TI; - Gerenciamento do Portifólio de Serviços; - Gerenciamento da Demanda.	
Desenho de Serviço	- Gerenciamento do Catálogo de Serviços; - Gerenciamento do Nível de Serviço; - Gerenciamento da Capacidade; - Gerenciamento da Disponibilidade; - Gerenciamento da Continuidade de Serviço; - Gerenciamento de Segurança da Informação; - Gerenciamento de Fornecedor.	
Transição de Serviço	- Gerenciamento de Mudança; - Gerenciamento da Configuração e de Ativo de Serviço; - Gerenciamento da Liberação e Implantação; - Validação e Teste de Serviço; - Avaliação; - Gerenciamento do Conhecimento.	
Operação de Serviço	- Gerenciamento de Evento; - Gerenciamento de Incidente; - Cumprimento de Requisição; - Gerenciamento de Problema; - Gerenciamento de Acesso.	- Central de Serviço; - Gerenciamento Técnico; - Gerenciamento das Operações de TI; - Gerenciamento de Aplicativo.
Melhoria de Serviço Continuada	- Relatório de Serviço; - Medição de Serviço.	

Tabela 2: Processos e Funções do ITIL v3, adaptado de OGCF, 2007

2.1. Estratégia de Serviços

O objetivo da Estratégia de Serviços é prover satisfação em necessidades particulares através da prestação de serviços, que devem ser baseada no princípio fundamental de que clientes esperam agregar valores que permitam atingir objetivos desejados. Segundo [FERNANDES, 2008, p.276], as seguintes questões são levantadas na estratégia de serviço:

- Quais serviços oferecer e para quem?
- Como se diferenciar dos competidores?
- De que forma é possível criar o conceito de valor de serviço, fazendo-o circular efetivamente entre os grupos interessados e os clientes?
- Como gerenciar os aspectos financeiros dos serviços?
- Como definir a qualidade do serviço, e como melhorá-la?
- Como alocar recursos de forma eficiente através de um portfólio de serviços, e como resolver conflitos de demanda entre eles?

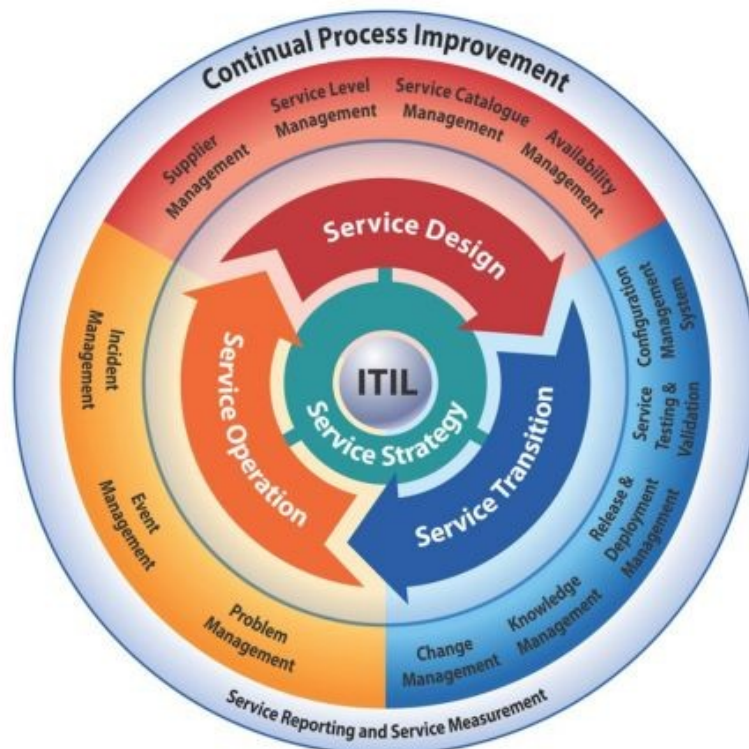


Figura 2: Ciclo de Vida do ITIL v3, Fonte OGCf, 2007

De acordo com a Figura 2, que apresenta o ciclo de vida do ITIL, a Estratégia de Serviços está no núcleo do ITIL, para apresentar aos provedores de serviços uma compreensão do que deve ser oferecido e para quem, como desenvolver o mercado interno e externo através de competitividade e diferenciais, como os clientes irão decidir pela contratação dos serviços e como se dará a obtenção e percepção de valor.

A Estratégia de Serviços não pode ser criada ou existir de forma isolada da estratégia e cultura da organização para a qual o provedor de serviços atua. O provedor pode existir em uma organização para prover serviços para um único ou vários departamentos, ou pode operar provendo serviços para múltiplas organizações externas. A estratégia adotada deve prover o valor esperado pelos clientes, de forma a atender o propósito estratégico do provedor de serviços.

2.2. Desenho de Serviços

Para que serviços agreguem valor real ao negócio, eles devem ser projetados com os objetivos de negócio em mente. É no desenho de serviço que as estratégias de serviços são transformadas em projetos de soluções tecnológicas que deverão entregar valor de acordo com os objetivos de negócio (OGCb, 2007, p.3).

O desenho de serviços emprega princípios de projetos e métodos para converter objetivos estratégicos em portfólio e ativos de serviços. O escopo do desenho de serviços não está limitado a apenas novos serviços, uma vez que compreende mudanças e melhorias necessárias para o aprimoramento e/ou manutenção dos serviços e do valor agregado ao negócio ao longo do ciclo de vida, da continuidade, do atendimento de metas e conformidade com padrões e regulamentações (OGCb, 2007, p.7).

Os tópicos-chave do desenho de serviços incluem o catálogo de serviços, disponibilidade, capacidade, continuidade e gerenciamento de níveis de serviços.

2.3. Transição de Serviços

A Transição de Serviços guia o provedor no desenvolvimento e melhoramento de capacidades para a transição de serviços novos ou modificados em um serviço operacional (OGCc, 2007, p.6).

Segundo (OGCc, 2007, p.7-8), é na Transição de Serviços que os requisitos de negócio, definidos na fase de Estratégia de Serviços e transformados em projetos pela fase de Desenho de Serviços, são efetivamente realizados em Operações de Serviços, controlando os riscos de falhas e interrupções.

Nesta fase, o sistema de gerenciamento de conhecimento sobre serviços é utilizado para a tomada de decisão sobre a gestão de serviços com base nos dados e informações atualizadas sobre configuração, capacidade, erros conhecidos, biblioteca de mídia definitiva e ativos.

2.4. Operação de Serviços

É na Operação de Serviços que as práticas de gestão do dia-a-dia são aplicadas para alcançar efetividade e eficiência na entrega e suporte a serviços, de forma a garantir a entrega de valor ao cliente e ao provedor de serviços. Os objetivos estratégicos são atingidos através da Operação de Serviços, tornando-a uma capacidade crítica para o negócio (OGCd, 2007, p.9-10,15).

Os gerentes e operadores de serviços, através dos processos e ferramentas podem tomar melhores decisões em áreas como o gerenciamento da disponibilidade, da demanda, otimização da utilização da capacidade, operacionalização e resolução de problemas.

2.5. Melhoria Continuada de Serviços

A melhoria continuada de serviços guia os provedores na criação e manutenção de valor para os clientes através de melhores projetos, transições e operações de serviços através da combinação de práticas e métodos de gerenciamento e melhoria da qualidade e capacidade.

O objetivo da melhoria continuada é proporcionar a organização a realização de melhorias incrementais e de grande escala na qualidade do serviço, na eficiência operacional e continuidade do negócio.

No ITIL, a melhoria continuada de serviços é composta por três componentes principais (OGCe, 2007, p.54-57):

- i. O Processo de Melhoria em 7 Passos, ilustrado na Figura 3;
- ii. As métricas de serviços, que definem os resultados esperados dos serviços de TI;
- iii. Relatórios de serviços, que apresentam uma visão analítica do estado de adequação as métricas estabelecidas para os serviços de TI.

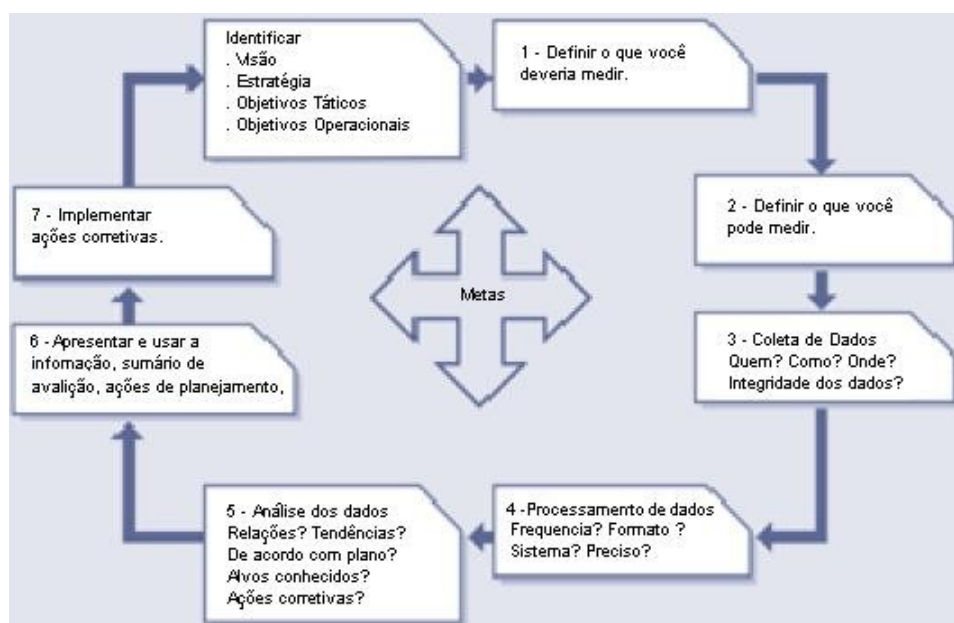


Figura 3: O processo de melhoria em 7 passos, adaptado de OGCE, 2007

Parece óbvio como as atividades do processo de melhoria ajudam a melhoria continuada de serviços (OGCE, 2007, p.38). É realmente simples identificar cada passo, mas a dificuldade reside em entender exatamente como isso irá ocorrer. O processo de melhoria abrange não apenas a gestão da organização, mas todo o ciclo de vida do serviço, como pode ser visto nos passos detalhados abaixo:

1. Definir o que você deveria medir – Na concepção do serviço, a Estratégia de Serviço e o Desenho de Serviço deveriam identificar esta informação, desta forma, a melhoria continuada pode recomeçar até atingir a situação ideal para os negócios e a TI, respondendo a pergunta 'onde desejamos chegar?';
2. Definir o que você pode medir – Esta atividade está relacionada com a pergunta 'onde desejamos chegar?'. Através da identificação dos níveis de serviço desejados pelo negócio, as capacidades de TI (identificadas pelo Desenho de Serviço e implementadas através da Transição de Serviços) e orçamentos disponíveis. A melhoria continuada realiza uma análise de deficiências para identificar novas oportunidades de melhoria, cujo foco é responder a 'onde desejamos chegar?';
3. Coleta de dados – Para responder a pergunta 'atingimos o objetivo?', os dados devem ser obtidos (através da Operação de Serviços) baseados nos objetivos e metas identificados. Estes são a entrada do próximo passo;

4. Processamento de dados – Neste passo, os dados coletados são processados em conformidade com os fatores críticos de sucesso e indicadores principais para o negócio. O objetivo deste passo é produzir dados estruturados para análise futura;
5. Análise dos dados – Os dados estruturados são transformados em informações sobre os serviços. A medida que são analisados, as oportunidades de melhorias, tendências e impacto nos negócios são identificadas. Este passo geralmente é esquecido ou realizado de maneira inadequada com a pressa em apresentar dados a gerência (OGCe, 2007, p.39);
6. Apresentar e usar informação – Aqui a resposta a pergunta 'nós chegamos lá?' é formatada e apresentada aos interessados com uma visão exata dos resultados dos esforços de melhoria realizados. Os resultados são apresentados ao negócio de forma a refletir suas necessidades e auxiliar na determinação dos próximos passos;
7. Implementar ações corretivas – O conhecimento obtido é usado para otimizar, melhorar e corrigir os serviços. Os gerentes de serviços identificam os problemas e apresentam soluções, as ações corretivas necessárias são comunicadas e explicadas a organização e uma nova *baseline* é estabelecida, recomeçando o ciclo.

Capítulo 3 – A Metodologia ISO/IEC 27002

No capítulo anterior, foi apresentada uma visão geral das melhores práticas para a gestão de serviços de TI através do ITIL. Neste capítulo, será apresentada uma introdução às melhores práticas para a gestão da segurança da informação através da ISO/IEC 27002:2005.

As organizações e seus sistemas de informação estão sendo cada vez mais exigidos, com riscos e incertezas de uma ampla variedade de fontes, incluindo o vírus de computador, fraudes, espionagem, sabotagem, vandalismo, incêndios ou inundações (NIST, 2006, p.5). Vírus e ataques de intrusão ou negação de serviços estão se tornando cada vez mais comuns, ambiciosos e sofisticados (ISO/IEC 27002, 2005, p.1).

A segurança da informação é importante, tanto no setor público e privado, para proteger infra-estruturas críticas. Em ambos os setores, a segurança da informação viabilizará, por exemplo, realizar comércio ou governo eletrônico, evitando e reduzindo os riscos relevantes. A interligação das redes públicas e recursos privados e o compartilhamento de informação aumentam a dificuldade de garantir o controle de acesso (ISO/IEC 27002, 2005, p.1). A tendência para a computação distribuída dificulta a eficácia do controle central e especializados (BELAPURKAR et al., 2009, p.15).

Muitos sistemas de informação não foram projetados para serem seguros. A segurança que se pode alcançar através de meios técnicos é limitada, e deve ser apoiada por uma gestão clara e procedimentos bem definidos. A identificação e aplicação de controles necessários dependem de planejamento cuidadoso e atenção aos detalhes. A gestão de segurança da informação exige uma participação mínima de todos os níveis funcionais da organização, podendo inclusive exigir a participação de fornecedores, clientes ou acionistas. Muitas vezes, a consultoria de agentes externos especializados também pode ser necessária (ISO/IEC 27002, 2005, p.15).

Com origem no Governo Britânico, a norma BS7799 é a base para a norma ISO/IEC 17799 que veio a tornar-se ISO/IEC 27002. O Código de Boas Práticas ISO/IEC 27002 fornece uma estrutura para avaliar os sistemas de gestão de segurança da informação baseada em um conjunto de diretrizes e princípios que têm sido adotadas por empresas, governos e organizações empresariais em todo o mundo.

A ISO/IEC 27002 utiliza fortemente o ciclo de Planejamento, Execução, Controle e Ação (PDCA da sigla em inglês) idealizado por Shewhart e mais tarde aplicado por Deming (FERNANDES, 2008, p.353). O ciclo é composto por um conjunto de ações em sequência, dada pela ordem estabelecida pelas letras que compõem a sigla: P (*plan*: planejar), D (*do*: fazer,

executar), C (*check*: verificar, controlar), e finalmente o A (*act*: agir, atuar corretivamente). Na Figura 4, é apresentado o ciclo PDCA como proposto pela ISO/IEC 27002 para sistemas de gerenciamento de segurança da informação.

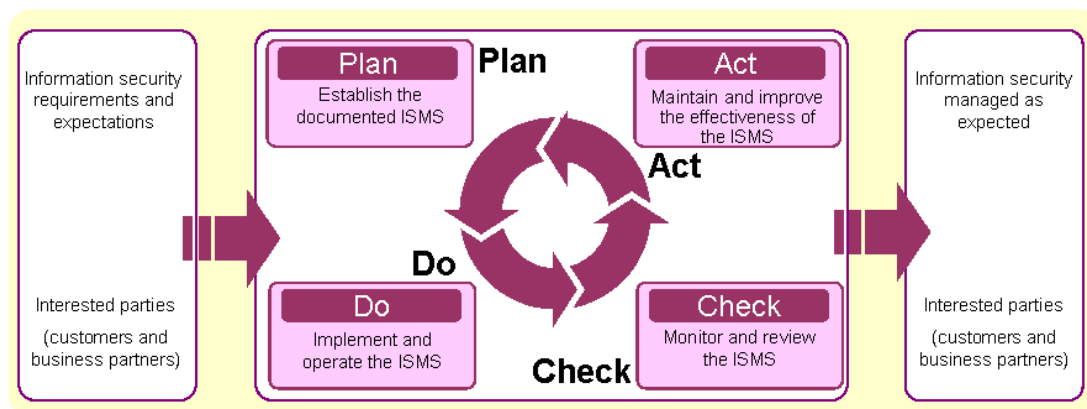


Figura 4: Modelo PCDA como usado em SGSI, Fonte ISO/IEC 27002

A Figura 4 mostra que, a partir dos requisitos de segurança da informação e de um conjunto de expectativas de clientes e outros interessados, é estabelecido um ciclo de planejamento, execução, verificação e melhoria que transforma as expectativas em resultados efetivamente implementados.

O *framework* de controles ISO permite aos profissionais de segurança da informação ter uma abordagem consistente e metódica, ao avaliar os processos de segurança nas organizações, infraestrutura de tecnologia, ou processos.

Os benefícios da segurança da informação estão na prevenção de perdas financeiras que a empresa pode ter, no caso da ocorrência de riscos de segurança da informação. Para que um sistema de informação seja considerado seguro, deve atender a quatro características:

- Integridade – A informação só poderá ser modificada por quem está autorizado e de maneira controlada;
- Confidencialidade – A informação só deverá estar disponível para quem está autorizado;
- Disponibilidade – A informação deverá estar disponível quando for necessária;
- Não repúdio – O uso ou modificação da informação por parte de uma pessoa autorizada deve ser irrefutável, ou seja, a pessoa não poderá negar a ação.

A norma ISO/IEC 27002 está estruturada em onze seções, cada uma destas é constituída por categorias de segurança da informação, sendo que cada categoria tem um objetivo de controle definido, um ou mais controles que podem ser aplicados para atender ao objetivo de controle, as

descrições dos controles, as diretrizes de implementação e informações adicionais.

Ao todo, são 133 controles divididos em (1) política de segurança da informação, (2) organização da segurança da informação, (3) gestão de ativos, (4) segurança em recursos humanos, (5) segurança física e de ambiente, (6) gerenciamento das operações e comunicações, (7) controle de acesso, (8) aquisição, desenvolvimento e manutenção de sistemas de informação, (9) gerenciamento de incidentes de segurança da informação, (10) gerenciamento da continuidade do negócio e (11) conformidade legal. Este trabalho não tem por objetivo explicitar todos estes controles, haja visto que a norma em si é fonte principal de informação para implementação destes controles.

O objetivo da **política de segurança da informação** é fornecer orientação e apoio às ações da gestão de segurança da informação sobre os requisitos de negócios e as leis e regulamentos pertinentes. A gerência deve estabelecer uma política clara e de acordo com os objetivos do negócio e demonstrar seu apoio e comprometimento com a segurança da informação através da publicação e manutenção de uma política segurança da informação para toda a organização (ISO/IEC 27002, 2005, p.12).

A **organização da segurança da informação** deve estabelecer uma estrutura de gestão a fim de iniciar e monitorar a implementação da segurança da informação dentro da organização. A administração deve adotar a política de segurança da informação, atribuir funções de segurança e de coordenação, bem como fiscalizar a execução da política de segurança em toda a organização. Se necessário, a organização deve estabelecer e facilitar o acesso às fontes de referência especializadas para garantir a atualização dos envolvidos sobre as tendências do setor, a evolução das normas e métodos de avaliação, e fornecer as ferramentas adequadas para a manipulação de resultados segurança. Seu objetivo deve ser a promoção de uma abordagem multi-disciplinar para a segurança da informação, que, por exemplo, envolva a cooperação e colaboração dos gestores, usuários, administradores, *designers* de aplicação, auditores e especialistas em segurança da informação, em áreas como gestão segurança e de riscos (ISO/IEC 27002, 2005, p.15).

A **gestão de ativos** tem por objetivo, alcançar e manter uma política de proteção adequada para os ativos da organização. Para que isso seja possível, devem ser identificados os proprietários para todos os ativos e atribuir a responsabilidade pela manutenção de controles adequados. A implementação de controles específicos pode ser delegada pelo proprietário caso seja conveniente. No entanto, o proprietário continua responsável pela proteção adequada dos ativos. O termo “prriprietário” identifica um indivíduo ou entidade responsável, com a aprovação dos mecanismos de direção, para controlar a produção, desenvolvimento, manutenção, utilização e segurança de ativos (ISO/IEC 27002, 2005, p.32).

Na **segurança em recursos humanos**, o objetivo é garantir que os funcionários, fornecedores e usuários de terceiros entendam suas responsabilidades, e esteja aptos a desempenhar suas funções, além de reduzir o risco de roubo, fraude e mau uso de recursos. As responsabilidades de segurança devem ser definidas antes da contratação, com a descrição adequada do trabalho e suas condições. Todos os funcionários, prestadores e usuários de terceiros devem ser selecionados adequadamente, especialmente para trabalhos sensíveis com acesso a informações. Funcionários, fornecedores e usuários de prestadores de serviços de processamento de informações devem assinar um acordo sobre seus papéis e responsabilidades relacionadas com a segurança (ISO/IEC 27002, 2005, p.38).

Para a **segurança física e de ambiente**, o objetivo é impedir o acesso físico não autorizado, dano ou interferência nas instalações e informações da organização. Os serviços de processamento de informações sensíveis devem ser realizados em áreas seguras e protegidas, em um perímetro de segurança definido por barreiras e controles de entrada adequada. Estas áreas devem ser fisicamente protegidas contra acesso não autorizado, danos e interferências. A proteção fornecida deve ser proporcional aos riscos identificados. Para evitar a perda, dano, roubo ou comprometimento de ativos e interrupção das atividades da organização, os equipamentos devem ser protegidos contra ameaças físicas e ambientais. A proteção dos equipamentos é necessária para reduzir o risco de acesso não autorizado à informação e à proteção contra perda ou roubo. Da mesma forma, deve-se a considerar controles especiais para proteção contra ameaças contra estruturas físicas e a garantia de serviços como eletricidade e infra-estrutura local (ISO/IEC 27002, 2005, p.47).

Com o **gerenciamento das operações e comunicações**, o objetivo é garantir a operação correta e segura dos recursos de tratamento de informação, estabelecendo responsabilidades e procedimentos para a gestão e operação de todos os recursos para o processamento de informações, incluindo o desenvolvimento de instruções e procedimentos operacionais de resposta a incidentes, implementando a segregação de funções, conforme o caso, para reduzir o risco de uma má utilização do sistema deliberadamente ou por negligência. A organização deve ainda implementar e manter um nível apropriado de controle e segurança nos serviços prestados por terceiros, de acordo como estabelecido em contratos pertinentes (ISO/IEC 27002, 2005, p.59).

O **controle de acesso** deve gerir o acesso à informação, recursos e processos de negócios com base nas necessidades de segurança e do negócio da organização. A regulamentação para as políticas de controle de acesso deve considerar a distribuição das informações e autorizações, devendo para isso, estabelecer procedimentos para atribuição de permissões de acesso aos sistemas e informações (ISO/IEC 27002, 2005, p.98).

A **aquisição, desenvolvimento e manutenção de sistemas de informação** deve garantir que a segurança é parte integral dos sistemas de informação. Os sistemas de informação incluem sistemas operacionais, infra-estrutura, aplicações de negócio, aplicações de uso geral, serviços e aplicações desenvolvidas pelos usuários. A concepção e implementação de sistemas de informação que dão apoio aos processos de negócio das empresas podem ser cruciais para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação. Todos os requisitos de segurança devem ser identificados na fase de levantamento de requisitos de um projeto e ser justificados, documentados e aceitos como parte de todo o processo para um sistema de informação (ISO/IEC 27002, 2005, p.127).

O **gerenciamento de incidentes de segurança da informação** deve garantir que os eventos e falhas de segurança associados aos sistemas de informação sejam identificados e comunicados o mais breve possível, permitindo assim a elaboração de medidas corretivas oportunas. Todos os funcionários, fornecedores e terceiros devem estar cientes dos procedimentos de comunicação de diferentes tipos de eventos e pontos fracos que possam ter impacto sobre a segurança dos ativos organizacionais (ISO/IEC 27002, 2005, p.148).

O **gerenciamento da continuidade do negócio**, deve implementar um processo de gestão da continuidade do negócio para reduzir a níveis aceitáveis, as perturbações causadas por catástrofes e falhas de segurança, através de uma combinação de controles preventivos e de recuperação, reagindo a interrupção das atividades de negócios. Para isto, é necessário identificar os processos críticos de negócio, e integrar os requisitos de gestão da segurança da informação e continuidade de negócios, com outros requisitos relacionados a aspectos tais como operações, fornecedores, funcionários, materiais, transporte e instalações (ISO/IEC 27002, 2005, p.156).

A **conformidade legal** tem por objetivo, evitar a violação de qualquer lei, estatuto, regulamento ou obrigações contratuais e de quaisquer requisitos de segurança. A concepção, funcionamento, utilização e gestão dos sistemas de informação podem estar sujeitos a requisitos legais, de segurança regulamentares e contratuais. Os requisitos legais específicas devem ser aconselhados por um advogado da organização ou profissionais qualificados (ISO/IEC 27002, 2005, p.163).

Isto posto, a ISO/IEC 27002:2005 pode ser vista como um ponto de partida para desenvolver uma gestão de segurança específica em uma organização. É importante observar que nem todas as recomendações e controles do referido código são aplicáveis a todos os tipos de organização e haverá casos onde controles adicionais possam ser necessários, muito embora não façam parte deste conjunto de recomendações e controles.

Capítulo 4 – A Metodologia COBIT

Nos últimos capítulos, foram apresentadas as melhores práticas para a gestão de serviços de TI e de segurança da informação. Neste capítulo, será apresentado um *framework* de melhores práticas para governança de TI.

Executivos precisam de garantias de que podem confiar em sistemas de informação e nas informações produzidas por esses sistemas, além de obter um retorno positivo dos investimentos feitos em TI. O COBIT permite aos executivos de negócios entenderem melhor como dirigir e gerenciar o uso da TI da empresa e os princípios de boas práticas que devem esperar de fornecedores de TI. O COBIT fornece as ferramentas para orientar e supervisionar todas as atividades relacionadas a TI.

Na Tabela 3, são apresentadas as perspectivas e metas de negócio que dirigem as ações de TI para atingir os objetivos de negócios e governança.

Metas de Negócios	Perspectiva Financeira	Prover um bom retorno de investimento nos negócios capacitados por TI
		Gerenciar os riscos de TI relacionados aos negócios
		Melhorar a governança corporativa e a transparência
	Perspectiva do Cliente	Melhorar a orientação ao cliente e serviços
		Oferecer produtos e serviços competitivos
		Garantir a disponibilidade e a continuidade dos serviços
		Demonstrar agilidade quando responder a mudanças de requisitos de negócios
		Garantir a otimização dos custos de entrega de serviço
		Obter informações confiáveis e úteis para a tomada de decisão
	Perspectiva Interna	Melhorar e manter as funcionalidades dos processos de negócios
		Diminuir os custos de processos
		Garantir a conformidade com leis, contratos e regras externas
		Garantir a conformidade com as políticas internas
		Gerenciar mudanças de negócios
		Melhorar e manter a produtividade operacional e da equipe
	Perspectiva de Aprendizado e Crescimento	Demonstrar a inovação de produtos/negócios
		Obter e manter pessoal capacitado e motivado

Tabela 3: Como a governança e os negócios dirigem a TI, adaptado de ITGIb, 2007

O COBIT ajuda a diminuir as distâncias entre os riscos do negócio, as necessidades de controle e questões técnicas (ITGIb, 2007, p.10). O COBIT define claramente a propriedade e responsabilidade orientado nos processos de negócio, permitindo um mapeamento dos objetivos de negócio, bem como o mapeamento de objetivos de TI em objetivos de processos (ITGIb, 2007, p.10).

As metas de negócios estão relacionadas as metas de TI, que consequentemente, estão relacionadas com os processos de TI. Desta forma, partindo de uma meta de negócio (Tabela 4 do Anexo I), é possível definir as metas de TI e os processos relacionados (Tabela 5 do Anexo II). Uma vez definidos os processos de TI, é possível identificar os objetivos de controle para a governança, métricas e orientações para o gerenciamento.

As Tabelas 4 e 5 dos Anexos I e II respectivamente, foram construídas com base no COBIT e podem ser utilizadas para definir quais processos devem ser implementados e/ou aprimorados para atender as metas de negócios. Para utilizar esta ferramenta, basta definir quais são as metas de negócios (Tabela 4 do Anexo I) e verificar quais são as metas de TI associadas. Uma vez identificadas as metas de TI que suportam as metas de negócios, é possível identificar quais processos de TI devem ser implementados ou melhorados (Tabela 5 do Anexo II). Os processos de TI apresentados são os 34 processos do COBIT descritos no Anexo III.

Uma vez identificados os processos de TI que segundo o COBIT precisam ser implementados na empresa, é possível utilizar o mapeamento para processos do ITIL ou ISO/IEC 27002 como descrito em (ITGIc, 2008) e (ITGIa, 2008), facilitando assim a execução das atividades técnicas pelas equipes operacionais. Desta forma, a implementação dos três *frameworks* será simplificada, reduzindo o tempo de planejamento e execução das atividades inerentes.

Sumarizando, os recursos de TI são gerenciados por procesos de TI para atingir objetivos de TI que respondem a requisitos de negócios. Este é o princípio básico do framework COBIT, como ilustrado no Cubo do COBIT na Figura 5.

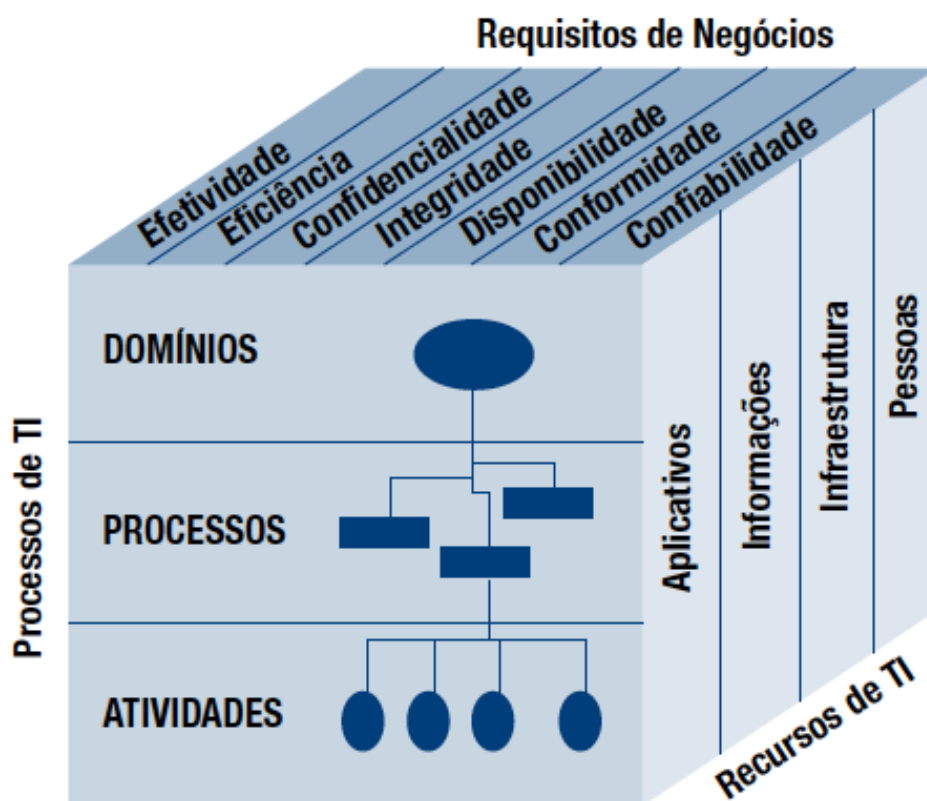


Figura 5: Os domínios do COBIT, adaptado de ITGIb, 2007, p.27

O cubo mostra em uma perspectiva estática três dimensões. A primeira apresenta os principais requisitos de negócios, esperados por boa parte das organizações empresariais. A segunda, organiza os processos de TI que irão atender aos requisitos de negócios em três níveis: o nível de **Domínios** inclui quatro grupos, (1) planejar e organizar, (2) adquirir e implementar, (3) entregar e suportar e (4) monitorar e avaliar; **Processos** que incluem 34 processos nos quatro domínios, cada um com um objetivo de controle de alto nível; e **Atividades** que são as ações necessárias para alcançar resultados mensuráveis. A terceira dimensão, Recursos de TI, contempla os recursos necessários para viabilizar os requisitos através dos processos de TI.

O *framework* COBIT, a partir de uma perspectiva dinâmica, apresenta suas atividades em uma estrutura lógica e gerenciável. Os processos de TI são organizados em quatro domínios e 34 processos. O framework identifica sete critérios de informação – efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade – relacionados com necessidades de negócio, além de ligações para os processos e diretrizes de gerenciamento para os administradores do negócio. Os recursos de TI são utilizados pelos processos de TI de forma a suportarem os objetivos de negócio.

O COBIT fornece as melhores práticas e ferramentas de monitoramento e gestão das atividades de TI. O uso de TI é um investimento significativo que precisa ser gerenciado. O COBIT ajuda os executivos a compreender e controlar os investimentos de TI em todo o seu ciclo de vida e fornece um método para avaliar se os serviços de TI e novas iniciativas estão reunindo os requisitos de negócio e são aptos a oferecer os benefícios esperados.

Uma visão gráfica mais detalhada do COBIT pode ser vista na Figura 6, com o modelo de processos do COBIT de quatro domínios e 34 processos genéricos, gerenciando os recursos de TI de forma a entregar informações aos negócios de acordo com os requisitos de negócios e governança.

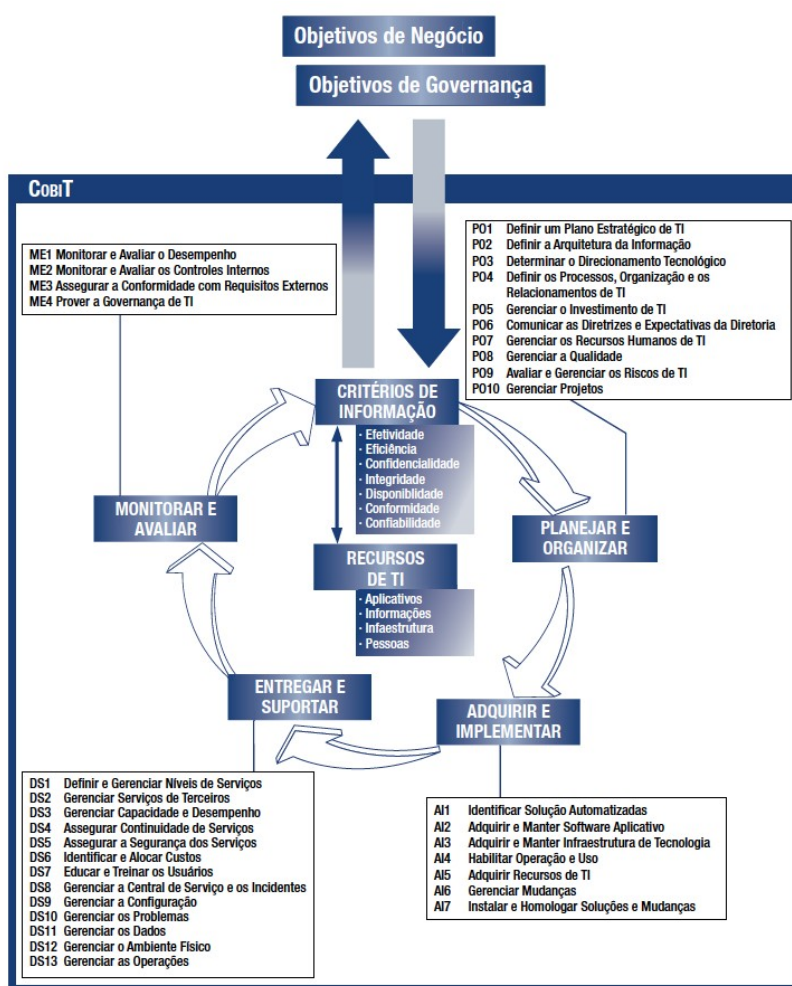


Figura 6: O modelo de governança COBIT, adaptado de ITGIB, 2007, p.28

Uma vez que o COBIT é um conjunto de ferramentas e técnicas aceitas internacionalmente, sua implementação é sinal de uma organização bem administrada. Ele ajuda os profissionais de TI e os usuários da empresa a demonstrarem a sua competência profissional para a gerência. Como

acontece com muitos processos de negócios genéricos, existem normas específicas no setor de TI e de boas práticas que as empresas devem seguir na utilização da TI. O COBIT capta essas melhores práticas e fornece um *framework* para a implementação e gestão (ITGlb, 2007, p.14).

Uma vez que os princípios fundamentais do COBIT relevantes a uma empresa são identificadas e implementados, os executivos ganham a confiança que o uso de TI pode ser gerido de forma eficaz. Os executivos podem esperar os seguintes resultados a partir da adoção do COBIT (ITGlb, 2007, p.10):

- A equipe de TI e os executivos irão compreender melhor como o negócio e a TI podem trabalhar juntos para entrega com sucesso de serviços de TI.
- O custo do ciclo de vida completo de TI tornar-se-á mais transparente e previsível.
- Irá proporcionar uma melhor qualidade e mais informações oportunas.
- Irá oferecer serviços de melhor qualidade e mais projetos de sucesso.
- Segurança e privacidade serão mais claros e a implementação mais facilmente controlável.
- Os riscos da TI serão geridos de forma mais eficaz.
- As auditorias serão mais eficientes e bem sucedidas.
- A observância dos requisitos regulamentares será uma prática comum de gestão.

O *framework* COBIT, nas versões 4.0 e superiores, incluem as seguintes características:

- **Framework** - Explica como o COBIT organiza a gestão de governança e objetivos de controle e de boas práticas por domínios e processos de TI, e suas ligações as necessidades do negócio. O *framework* contém um conjunto de 34 objetivos de controle de alto nível, uma para cada processo de TI, agrupados em quatro domínios: Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar, e Monitorar e Avaliar;
- **Descrições de processos** - Incluídos para cada um dos 34 processos de TI, abrangendo as áreas de responsabilidade do negócios e de TI do começo ao fim;
- **Objetivos de controle** - Fornece objetivos genéricos de melhores práticas de gestão de processos de TI;
- **Diretrizes de Gestão** - Oferecem ferramentas para ajudar a atribuir responsabilidades e medir o desempenho;

- **Modelos de Maturidade** - Fornece perfis de processos de TI descrevendo possíveis estados atuais e futuros.

O processo de implementação do COBIT consiste em alguns passos, que começam com a introdução dos objetivos de negócios na ótica do *framework*. Uma vez que as metas são conhecidas, é possível determinar quais processos de TI e seus respectivos controles devem ser empregados para suportar o negócio. É importante ressaltar que, antes de iniciar o processo de implementação, é essencial o pleno conhecimento das estratégias do negócio onde o planejamento estratégico, ou mesmo o plano de negócios são as principais fontes.

Os processos de TI e seus resultados devem ser avaliados utilizando as diretrizes de auditoria correspondentes, de forma que seja possível garantir que os resultados obtidos estão de acordo com o que é esperado. Através do monitoramento constante do desempenho e com o auxílio das diretrizes de gestão dos processos de TI, será possível identificar e priorizar as atividades críticas dentro da organização, permitindo assim alcançar as metas de negócio.

No Anexo IV é apresentado um Plano de Ações genérico que pode ser aplicado nas organizações para guiar a implementação da Governança de TI segundo a ótica do COBIT, e sua interligação com os *frameworks* ITIL e ISO/IEC 27002:2005 através do mapeamento de processos destes disponível em (ITGIa, 2007).

Apesar de possuir um nível adequado de detalhes, o ITIL não atende a todos os aspectos da Governança e Gestão de Serviços de TI como é tratado no COBIT. Os processos do domínio Entregar e Suportar do COBIT são cobertos de forma extensiva, enquanto os processos, atividades e responsabilidades dos domínios Planejar e Organizar, Adquirir e Implementar, Monitorar e Avaliar não são tratados adequadamente pelo ITIL. No mesmo aspecto, a ISO/IEC 27002:2005 provê métricas genéricas para a gestão da segurança da informação e conformidade regulamentar e de legislação. Com foco em problemas da segurança, não atende a todo o escopo da gestão de TI.

Enquanto o COBIT e a ISO/IEC 27002 definem o que deve ser feito, o ITIL define como deve ser feito, criando assim uma sinergia entre as melhores práticas. As Tabelas 6 e 7 dos Anexos V e VI apresentam as relações entre os processos do COBIT/ITIL e ISO/IEC 27002/ITIL respectivamente, e servem como uma visão geral da interação entre os *frameworks*.

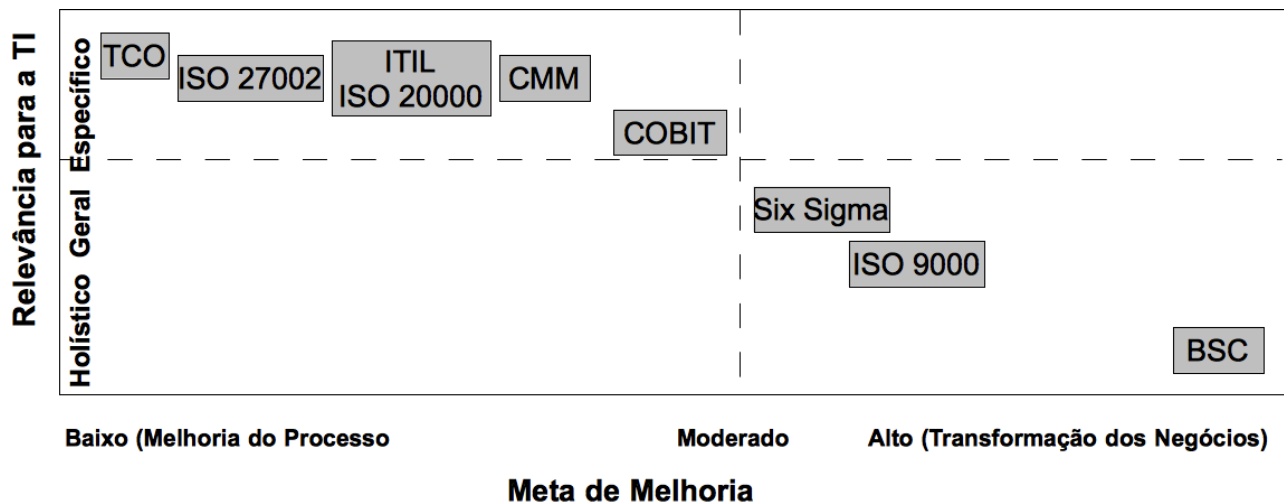


Figura 7: COBIT e outros padrões, do autor

A relevância de padrões e práticas depende da organização e suas prioridades e expectativas. Uma organização pode decidir por adotar todos, um ou parte de um dos padrões para melhorar o desempenho de um processo de negócios ou permitir a transformação de negócios. A Figura 7 mostra o COBIT posicionado ao centro, ajudando a integrar as práticas técnicas e específicas de TI com as de negócios mais amplas. Ele está alinhado com outras melhores práticas e pode ser usado como o integrador de diferentes guias, como por exemplo a ISO/IEC 27002 e o ITIL, e por isso, é cada vez mais reconhecido internacionalmente como o *framework de facto* para a governança de TI (ITGIb, 2007, p.30).

Como o COBIT está alinhado a outros padrões, sendo geralmente aceito como um *framework* de controle e governança de TI, garantindo a conformidade com leis e regras relacionadas, torna a governança um processo natural para a TI e uma prática normal de negócios.

Conclusão

As organizações são desafiadas a adaptarem-se a demandas dinâmicas do mundo dos negócios, enquanto reduzem riscos e complexidades relacionadas a adoção de tecnologias, usadas para suportar o negócio a alcançar seus objetivos estratégicos.

A TI por sua vez, enfrenta desafios dentre os quais destaco: manter a TI funcionando, agregar valor ao negócio, reduzir custos e complexidades, alinhamento com as estratégias de negócio, atender a requisitos regulamentares e manter a segurança das operações.

Apesar da grande quantidade de benefícios trazidos pela implantação da governança de TI, não se deve esperar apenas benefícios em um processo dessa natureza, afinal em certos casos, algumas das medidas adotadas com certeza irão divergir com processos que anteriormente eram tidos como “corretos” pela empresa, usuários ou mesmo pelos profissionais envolvidos com as rotinas diárias de TI.

Dentre os problemas que certamente são enfrentados em um projeto de implementação da governança de TI em uma organização, pode-se destacar a (1) falta de investimentos adequados, (2) comprometimento e entendimento, (3) cultura da empresa, (4) excesso de expectativa, (5) problemas na gestão do projeto, e (6) Controle fraco ou incompatível com os objetivos do processo e do projeto.

Desta forma, fica claro que um bom planejamento e o apoio do alto escalão da empresa são fatores críticos de sucesso para um projeto desta natureza. Existem algumas precauções que são de vital importância para o sucesso da implementação:

- i. O projeto deve ter o apoio da alta administração da empresa, ou seja, a idéia deve ser apresentada e “vendida” para a alta administração antes de se iniciar a implantação. Toda mudança geralmente gera resistência e o melhor apoio contra esta resistência é a mudança ser uma decisão “superior”, ou seja, ter aprovação e apoio da alta gerência;
- ii. A cultura da empresa também é um fator que dificulta o processo de implementação. Para diminuir este impacto, além do apoio da alta gerência, é importante também que seja realizado um trabalho de divulgação e conscientização dos envolvidos sobre os benefícios que serão colhidos por todos a médio e longo prazo;
- iii. É importante alinhar as expectativas de todos os envolvidos no processo de implantação, usuários, profissionais de TI, alta gerência, etc;

- iv. Outro ponto chave para o sucesso de uma implantação da governança de TI em uma organização, é a definição clara do escopo e dos processos que serão implementados, buscando alinhar ao máximo os processos de TI com os objetivos do negócio, e evitando mudanças que prejudiquem os processos que geram maior receita para a organização.

Não há um único *framework* de governança de TI que atenda a todos os requisitos de uma organização, assim, os três apresentados devem ser utilizados em conjunto, de forma complementar, haja visto que COBIT é forte em controle e métricas, a ISO/IEC 27002 em segurança da informação, enquanto o ITIL é focado em processos, especialmente aqueles relacionados com central de serviços. Os três *frameworks* seguem o modelo PDCA de processos.

Resistir ao tecnicismo para não comprometer a aproximação entre TI e os negócios e tornar verdadeiramente transparente o desempenho de tecnologia, é o desafio dos gestores. Para não deixar escapar esta oportunidade ímpar de se integrar no nível estratégico de suas organizações através de uma comunicação clara e uma gestão transparente e assim influenciar o futuro da organização.

Para trabalhos futuros, uma oportunidade é estudar o nível de penetração das melhores práticas abordadas nas organizações, as dificuldades e desafios enfrentados, bem como nível de conformidade destas com as leis brasileiras.

Bibliografia

- BECKER** et al., Becker, João Luiz, Lunardi, Guilherme Lerch, Maçada, Antonio Carlos Gastaud. Relatório Executivo: Governança de TI e o Desempenho Organizacional. Universidade Federal do Rio Grande do Sul, 2007
- BELAPURKAR** et al. Distributed Systems Security: Issues, Processes and Solutions. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnappalli, Niranjana Varadarajan, Srinivas Padmanabhuni, Srikanth Sundarajan. Wiley, 2009
- BERNARDES**, Mauro Cesar e **MOREIRA**, Edson dos Santos. Um Modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional. São Paulo. Universidade de São Paulo, 2007
- FERNANDES**, Aguinaldo Aragon. Implantado a governança de TI: da estratégia a gestão dos processos e serviços / Agnaldo Aragon Fernandes, Vladimir Ferraz de Abreu. 2. ed. Rio de Janeiro: Brasport, 2008
- FTC**, Federal Trade Commission. Privacy Online: Fair Information Practices in the Electronic Marketplace. Federal Trade Commission, 2000
- ISACA**, COBIT Handbook. Information Systems Audit and Control Association, 2007
- ISO/IEC 20000-1:2005**. Information Technology – Service Management – Part 1: Code of practice, 2005. International Organization for Standardisation
- ISO/IEC 27001:2005**: Information technology – Security techniques – Information security management systems – Requirements, first edition, 2005. International Organization for Standardisation
- ISO/IEC 27002:2005**: Information technology – Security techniques – Code of practice for information security management, 2005. International Organization for Standardisation
- ITGIa**, Information Technology Governance Institute. Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit, Information Technology Governance Institute, Office for Government Commerce, 2008
- ITGIb**, Information Technology Governance Institute. COBIT 4.1. Information Technology Governance Institute, 2007
- ITGIc**, Information Technology Governance Institute. COBIT mapping: mapping of ITIL with

COBIT 4.1. Information Technology Governance Institute, Rolling Meadows, 2008

ITSMF, United Kingdom IT Service Management Forum <http://www.itsmf.com/bestpractices/>

MANSUR, Ricardo. Governança de TI: metodologia, frameworks e melhores práticas. Rio de Janeiro: Brasport, 2007

MODULO, Modulo Security. 10ª Pesquisa Nacional de Segurança da Informação. Modulo Security, 2006

NIST, National Institute of Standards and Technology: Information Security Handbook – A Guide for Managers. National Institute of Standards and Technology, 2006

OGCa, Office for Government Commerce: ITIL® - Service Strategy. The Stationary Office, 2007

OGCb, Office for Government Commerce: ITIL® - Service Design. The Stationary Office, 2007

OGCc, Office for Government Commerce: ITIL® - Service Transition. The Stationary Office, 2007

OGCd, Office for Government Commerce: ITIL® - Service Operation. The Stationary Office, 2007

OGCe, Office for Government Commerce: ITIL® - Continual Service Improvement. The Stationary Office, 2007

OGCf, Office for Government Commerce: ITIL® - The Official Introduction to the ITIL Service Lifecycle. The Stationary Office, 2007

OGCg, Office for Government Commerce: ITIL® - ITIL Official Website <http://www.itil.co.uk>

OGCh, Office for Government Commerce: OGC Official Website <http://www.ogc.gov.uk>

PARTHA et al.. Intrusion Tolerant Systems. Partha P. Pal, Franklin Webber, Richard E. Schantz and Joseph P. Loyall. Cambridge, 2000

PTACEK, Thomas H., NEWSHAM, Timothy N. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Secure Networks Inc, 1998

RFC2196, Internet Engineering Task Force. Site Security Handbook. Internet Engineering Task Force, 1997

WEILL, Peter e ROSS, Jeanne W. Governança de TI, Tecnologia da Informação. Tradução de Tereza Cristina M. B. Carvalho. São Paulo: M. Books, 2006

ANEXO I - Mapeamento de Metas de Negócios em Metas de TI

Metas de Negócios		Metas de TI										Eficácia	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade
Perspectiva Financeira	1. Prover um bom retorno de investimento nos negócios capacitados por TI	24											X					
	2. Gerenciar os riscos de TI relacionados aos negócios	2	14	17	18	19	20	21	22					X	X	X		
	3. Melhorar a governança corporativa e a transparência	2	18															X
Perspectiva do Cliente	4. Melhorar a orientação ao cliente e serviços	3	23									X						
	5. Oferecer produtos e serviços competitivos	5	24									X	X					
	6. Garantir a disponibilidade de serviço	10	16	22	23							X				X		
	7. Criar agilidade quando responder as mudanças de requisitos	1	5	25								X	X					
	8. Garantir a otimização do custo da entrega de serviço	7	8	10	24								X					
	9. Obter informações confiáveis e úteis para a tomada de decisão	2	4	12	20	26						X			X			X
Perspectiva Interna	10. Melhorar e manter as funcionalidades dos processos de negócios	6	7	11								X	X					
	11. Diminuir os custos de processos	7	8	13	15	24						X	X					
	12. Garantir a conformidade com leis, contratos e regras externas	2	19	20	21	22	26	27						X			X	
	13. Garantir a conformidade com as políticas internas	2	13															X
	14. Garantir mudanças de negócios	1	5	6	11	28								X			X	
	15. Melhorar e manter a produtividade operacional e da equipe	7	8	11	13							X	X					
Perspectiva de Aprendizado e Crescimento	16. Gerenciar inovações de produtos/negócios	5	25	28								X	X					
	17. Adquirir e manter pessoal capacitado e motivado	9										X	X					

Tabela 4: Mapeamento de metas de negócios em metas de TI, adaptado de ITGIb, 2007

ANEXO II - Mapeamento de Metas de TI em Processos de TI

Metas de TI	Processos de TI									
1. Responder aos requisitos de negócios em alinhamento com a estratégia de negócios	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1
2. Responder aos requisitos de governança alinhado com a direção do conselho	PO1	PO4	PO10	ME1	ME3					
3. Garantir a satisfação de usuários finais com ofertas de serviço e níveis de serviço	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13		
4. Otimizar o uso da informação	PO2	DS11								
5. Criar agilidade de TI	PO2	PO4	PO7	AI3						
6. Definir como os requisitos de negócios, funcionalidades e controles serão traduzidos para soluções automatizadas eficazes e eficientes	AI1	AI2	AI6							
7. Adquirir e manter sistemas de aplicações integrados e padronizados	PO3	AI2	AI5							
8. Adquirir e manter uma infraestrutura de TI integrada e padrinizada	AI3	AI5								
9. Adquirir e manter as habilidades de TI que respondem a estratégia de TI	PO7	AI5								
10. Garantir a satisfação mútua de relacionamentos de terceiros	DS2									
11. Integrar perfeitamente as aplicações e soluções de tecnologia para processos de negócios	PO2	AI4	AI7							
12. Garantir transparência e entendimento do custo de TI, benefícios, estratégia, políticas e níveis de serviço	PO5	PO6	DS1	DS2	DS6	ME1	ME4			
13. Garantir o uso apropriado e performance de aplicações e soluções de tecnologia	PO6	AI4	AI7	DS7	DS8					
14. Explicar e proteger todos os ativos de TI	PO9	DS5	DS9	DS12	ME2					

Tabela 5: Mapeamento de metas de TI em processos de TI, adaptado de ITGIb, 2007

ANEXO II - Mapeamento de Metas de TI em Processos de TI

Metas de TI	Processos de TI									
15. Otimizar a infraestrutura de TI, recursos e capacidades	PO3	AI3	DS3	DS7	DS9					
16. Reduzir defeitos e re-trabalho de solução e entrega de serviço	PO8	AI4	AI6	AI7	DS10					
17. Proteger o alcance dos objetivos de TI	PO9	DS10	ME2							
18. Estabelecer transparência do impacto de negócios de riscos para os objetivos e recursos de TI	PO9									
19. Garantir que informações críticas e confidenciais sejam retidas daqueles que não deveriam ter acesso a isso	PO6	DS5	DS11	DS12						
20. Garantir que transações automatizadas de negócios e trocas de informações possam ser confiáveis	PO6	AI7	DS5							
21. Garantir que os serviços de TI e infraestrutura possam resistir e se recuperar apropriadamente de falhas devido a erros, ataques deliberados ou desastres	PO6	AI7	DS3	DS5	DS12	DS13	ME2			
22. Garantir o mínimo impacto de negócios no evento de uma perturbação ou mudança	PO6	AI6	DS3	DS12						
23. Garantir que os serviços de TI estejam disponíveis conforme necessário	DS3	DS4	DS8	DS13						
24. Melhorar o custo-benefício da TI e a sua contribuição para os lucros dos negócios	PO5	AI5	DS6							
25. Entregar projetos em tempo e dentro do orçamento enquanto alcança padrões de qualidade	PO8	PO10								
26. Manter a integridade da informação e infraestrutura de processamento	AI6	DS5								
27. Garantir a conformidade de TI com leis e regras	DS11	ME2	ME3	ME4						
28. Garantir que a TI demonstre qualidade de serviço, custo-benefício, melhoria contínua e prontidão para futuras mudanças	PO5	DS6	ME1	ME3						

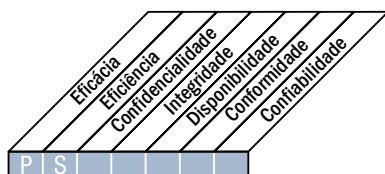
Tabela 5: Mapeamento de metas de TI em processos de TI, adaptado de ITGIb, 2007

ANEXO III – Descrições dos Processos do COBIT 4.1

DESCRIÇÃO DE PROCESSO

PO1 Definir um Plano Estratégico de TI

O planejamento estratégico de TI é necessário para gerenciar todos os recursos de TI em alinhamento com as prioridades e estratégias de negócio. A função de TI e as partes interessadas pelo negócio são responsáveis por garantir a otimização do valor a ser obtido do portfólio de projetos e serviços. O plano estratégico deve melhorar o entendimento das partes interessadas no que diz respeito a oportunidades e limitações da TI, avaliar o desempenho atual e esclarecer o nível de investimento requerido. A estratégia e as prioridades de negócio devem ser refletidas nos portfólios e executadas por meio de planos táticos de TI que estabeleçam objetivos concisos, tarefas e planos bem definidos e aceitos por ambos, negócio e TI.



Controle sobre o seguinte processo de TI:

Definir um plano estratégico de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

sustentar ou estender a estratégia de negócio e os requisitos de governança e, ao mesmo tempo, ser transparente quanto aos benefícios, custos e riscos.

com foco em:

incorporar TI e gerenciamento de negócio na tradução dos requisitos de negócio em ofertas de serviços e no desenvolvimento de estratégias para entregar estes serviços de maneira eficaz e transparente.

é alcançado por:

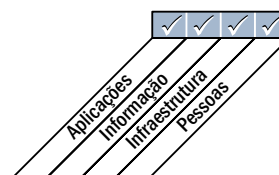
- Comprometimento da Alta Direção e da Direção do Negócio no alinhamento do planejamento estratégico de TI com as necessidades atuais e futuras;
- Entendimento da capacidade atual de TI;
- Estabelecimento de um esquema de priorização de objetivos de negócio, que quantifique os requisitos de negócio;

e medido por:

- Percentual dos objetivos de TI no plano estratégico de TI que sustentam o plano estratégico de negócio;
- Percentual de projetos no portfólio de projetos de TI que podem ser diretamente relacionados ao plano tático de TI;
- Demora entre a atualização do plano estratégico de TI e a atualização dos planos táticos de TI.



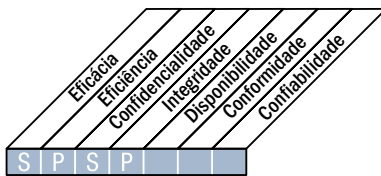
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

P02 Definir a Arquitetura da Informação

Os sistemas de informação devem criar e atualizar regularmente um modelo de informação do negócio e definir os sistemas apropriados para otimizar o uso dessa informação. Isso abrange o desenvolvimento de um dicionário de dados corporativo com as regras de sintaxe de dados, o esquema de classificação de dados e os níveis de segurança da organização. Esse processo melhora a qualidade de decisão do gerenciamento certificando-se de que informações seguras e confiáveis sejam fornecidas e permite racionalizar os recursos de sistemas de informação para atender às estratégias de negócio de forma apropriada. Esse processo de TI também é necessário para permitir um maior grau de responsabilização pela integridade e a segurança dos dados e melhorar a efetividade e o controle do compartilhamento da informação através das aplicações e entidades.



Controle sobre o seguinte processo de TI:

Definir a arquitetura da informação

que satisfaça aos seguintes requisitos do negócio para a TI:

ser ágil em atender aos requisitos, fornecer informação confiável e consistente e integrar completamente as aplicações nos processos de negócio

com foco em:

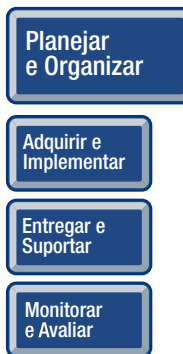
estabelecer um modelo de dados de negócio que incorpore um esquema de classificação de dados para assegurar integridade e consistência de todos os dados

é alcançado por:

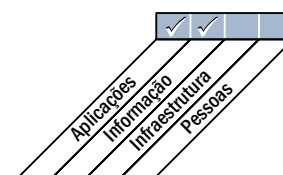
- Garantia da precisão da arquitetura da informação e do modelo de dados
- Estabelecimento da propriedade dos dados
- Classificação da informação utilizando um esquema de classificação acordado

e medido por:

- Percentual de elementos de dados redundantes ou duplicados
- Percentual de aplicações que não estão em conformidade com a arquitetura da informação
- Frequência de atividades de validação dos dados



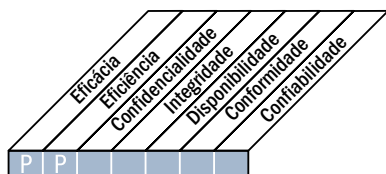
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

P03 Determinar as Diretrizes da Tecnologia

Os responsáveis pelos serviços de informação determinam um direcionamento tecnológico que suporta o negócio. Isso demanda a criação de um plano de infraestrutura tecnológica e um conselho de arquitetura que estabeleça e gerencie expectativas claras e realistas do que a tecnologia pode oferecer em termos de produtos, serviços e mecanismos de entrega. O plano é atualizado regularmente e abrange aspectos como arquitetura de sistemas, direcionamento tecnológico, plano de aquisições, padrões, estratégias de migração e contingência. Isso permite respostas rápidas a mudanças em um ambiente competitivo, economia de escala em equipes e em investimentos de sistemas de informação, bem como melhor interoperabilidade entre plataformas e aplicações.



Controle sobre o seguinte processo de TI:

Determinar as Diretrizes da Tecnologia

que satisfaça aos seguintes requisitos do negócio para a TI:

ter sistemas aplicativos, recursos e capacidades padronizados, integrados, estáveis, com boa relação custo-benefício, que atendam os requisitos atuais e futuros do negócio

com foco em:

definir e implementar um plano de infraestrutura, arquitetura e padrões de tecnologia que reconheça e aproveite as oportunidades tecnológicas

é alcançado por:

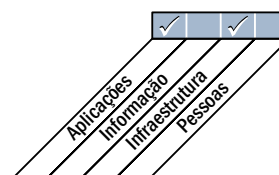
- Estabelecimento de um fórum para direcionar a arquitetura e verificar a sua conformidade;
- Estabelecimento de um plano equilibrado de infraestrutura tecnológica com relação aos requisitos, custos e riscos;
- Definição dos padrões de infraestrutura tecnológica com base nos requisitos da arquitetura da informação.

e medido por:

- Quantidade e tipo de desvios do plano de infraestrutura tecnológica
- Frequência de revisão/atualização do planejamento de infraestrutura tecnológica
- Quantidade de plataformas de tecnologia por área da organização



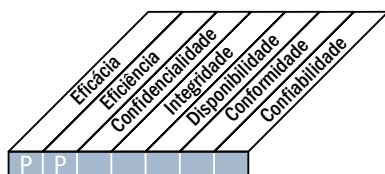
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

PO4 Definir os Processos, Organização e Relacionamentos de TI

Uma organização de TI é definida considerando os requisitos de pessoal, habilidades, funções, autoridade, papéis e responsabilidades, rastreabilidade e supervisão. Essa organização deve fazer parte de uma estrutura de processos de TI que assegure transparência e controle, assim como o envolvimento de executivos sênior e a Direção do negócio. Um comitê estratégico deve assegurar a supervisão da Direção de TI, e um ou mais comitês dos quais as áreas de negócio e TI participem devem definir a priorização dos recursos de TI em linha com as necessidades do negócio. Os processos, as políticas administrativas e os procedimentos precisam estar estabelecidos para todas as funções, com especial atenção às de controle, garantia da qualidade, gestão de risco, segurança da informação, propriedade de sistemas e dados e segregação de funções. Para assegurar o rápido atendimento das exigências do negócio, a TI deve ser envolvida nos processos de decisão relevantes.



Controle sobre o seguinte processo de TI:

Definir os processos, a organização e os relacionamentos de TI

que satisfaça aos seguintes requisitos de negócio para a TI:

ser ágil em resposta à estratégia de negócio e, ao mesmo tempo, atender aos requisitos de Governança e fornecer pontos de contatos definidos e competentes

com foco em:

estabelecer estruturas organizacionais de TI transparentes, flexíveis e responsivas e definir e implementar processos de TI com proprietários (de sistemas e dados), papéis e responsabilidades integrados aos processos de negócio e processos de decisão.

é alcançado por:

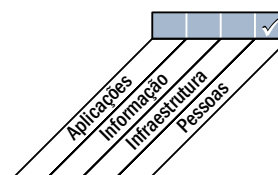
- Definição de uma estrutura de processos de TI
- Estabelecimento de conselhos e estruturas organizacionais apropriadas
- Definição de papéis e responsabilidades

e medido por:

- Percentual de funções com posições e descrições de autoridade documentadas;
- Número de unidades/processos de negócios não suportados pela organização de TI, mas que deveriam ser suportados de acordo com a estratégia;
- Número de atividades centrais de TI realizadas fora da organização de TI e que não são aprovadas ou submetidas aos padrões organizacionais de TI



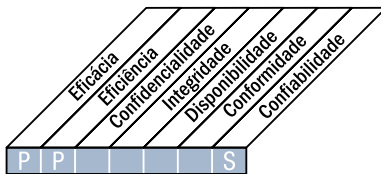
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

PO5 Gerenciar o Investimento de TI

Estabelecer e manter uma estrutura para gerenciar os programas de investimentos em TI que contemple custos, benefícios, prioridade dentro do orçamento, um processo formal de definição orçamentária e gerenciamento de acordo com o orçamento. As partes interessadas são consultadas para identificar e controlar os custos totais e os benefícios dentro dos contextos estratégicos e táticos da TI e iniciar ações de correção quando necessário. O processo promove a parceria entre a TI e as partes interessadas do negócio, permite o uso eficaz e eficiente dos recursos de TI, provê transparência, atribui responsabilidade pelo custo total de propriedade (TCO, *Total Cost of Ownership*), realização dos benefícios do negócio e do retorno sobre os investimentos em TI.



Controle sobre o seguinte processo de TI:

Gerenciar o investimento de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar continuamente e visivelmente a relação custo-benefício da TI e sua contribuição para a lucratividade do negócio com serviços integrados e padronizados que atendam às expectativas do usuário final.

com foco em:

decidir o portfólio e investimentos em TI de forma eficaz e eficiente e elaborar e rastrear os orçamentos de TI em linha com estratégias de TI e decisões de investimento

é alcançado por:

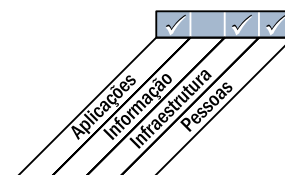
- Previsão e alocação de orçamentos
- Definição do critério de investimento formal (ROI – Retorno sobre Investimento, período de recuperação de investimento, NPV – Valor Presente Líquido)
- Medição e avaliação do valor de negócio comparado à previsão.

e medido por:

- Redução percentual do custo unitário dos serviços de TI entregues
- Percentual de desvio do valor orçamentário comparado com o orçamento total
- Percentual dos gastos de TI expressos através de motivadores de valor de negócio (por exemplo: aumento de vendas/serviços devido ao aumento da conectividade)



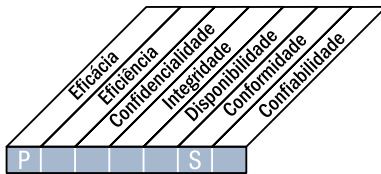
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

P06 Comunicar Metas e Diretrizes Gerenciais

A Direção deve desenvolver uma estrutura de controle de TI corporativo e definir e comunicar políticas. Um programa de comunicação contínuo aprovado e apoiado pela Direção deve ser implementado para articular missão, metas, políticas, procedimentos etc. A comunicação apoia o alcance dos objetivos de TI e assegura a consciência e o entendimento dos negócios, dos riscos de TI, dos objetivos e das diretrizes. O processo deve assegurar conformidade com leis e regulamentos relevantes.



Controle sobre o seguinte processo de TI:

Comunicar as diretrizes e expectativas da Diretoria

que satisfaça aos seguintes requisitos do negócio para a TI:

manter as informações precisas e atualizadas nos serviços de TI atuais e futuros, bem como as responsabilidades e os riscos associados

com foco em:

fornecer políticas, procedimentos, diretrizes e outras documentações de forma precisa, compreensível e aprovada para as partes interessadas, incorporada a uma estrutura de controles de TI

é alcançado por:

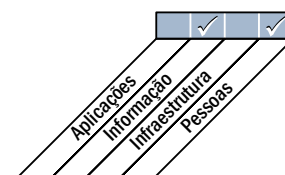
- Definição de uma estrutura de controle de TI
- Desenvolvimento e implementação de políticas de TI
- Imposição de políticas de TI

e medido por:

- Quantidade de interrupções no negócio devido a interrupções em serviços de TI
- Percentual de partes interessadas que entendem a estrutura corporativa de controle de TI
- Percentual das partes interessadas que não estão em conformidade com a política



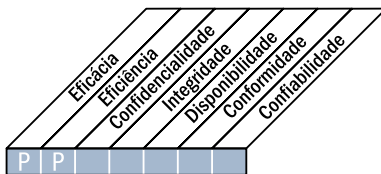
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

P07 Gerenciar os Recursos Humanos de TI

Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.



Controle sobre o seguinte processo de TI:

Gerenciar os Recursos Humanos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

ter pessoas competentes e motivadas para criar e entregar serviços de TI

com foco em:

admitir e treinar pessoal, motivar através de planos de carreira claros, atribuir funções coerentes com as habilidades, estabelecer um processo de revisão, criar descrições de cargos e assegurar a consciência da dependência de indivíduos.

é alcançado por:

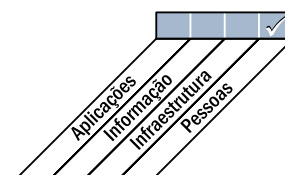
- Revisão do desempenho do pessoal
- Admissão e treinamento do pessoal de TI para sustentarem os planos táticos de TI
- Mitigar o risco de dependência excessiva de recursos-chave

e medido por:

- Nível de satisfação das partes interessadas com as experiências e habilidades da equipe de TI
- Rotatividade da equipe de TI
- Percentual da equipe de TI certificado de acordo com as necessidades da função



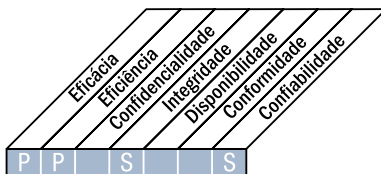
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

PO8 Gerenciar a Qualidade

Deve ser desenvolvido e mantido um sistema de gestão da qualidade, que inclua padrões e processos comprovados de desenvolvimento e aquisição. Isso é feito através de planejamento, implementação e manutenção de um sistema de gestão de qualidade que gere requisitos, procedimentos e políticas de qualidade claros. Requisitos de qualidade devem ser definidos e comunicados em indicadores quantificáveis e atingíveis. A melhoria contínua pode ser alcançada por constante monitoramento, análise e atuação sobre desvios e na comunicação dos resultados às partes interessadas. A gestão da qualidade é essencial para assegurar que a TI esteja fornecendo valor para o negócio, melhoria contínua e transparência para as partes interessadas.



Controle sobre o seguinte processo de TI:

Gerenciar a Qualidade

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar continuamente e de forma mensurável a qualidade dos serviços entregues pela TI

com foco em:

definir um sistema de gerenciamento de qualidade (SGQ), monitorar continuamente o desempenho baseado em objetivos predefinidos e implementar um programa de melhoria contínua dos serviços de TI

é alcançado por:

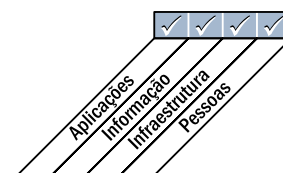
- Definição de práticas e padrões de qualidade
- Monitoração e revisão dos desempenhos interno e externo comparado às práticas e padrões de qualidade definidas
- Melhoria contínua do SGQ

e medido por:

- Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância)
- Percentual dos processos de TI formalmente revisados pelo processo de garantia de qualidade periodicamente e que atingem metas e objetivos de qualidade
- Percentual dos processos que recebem revisões de garantia de qualidade (QA-Quality Assurance)



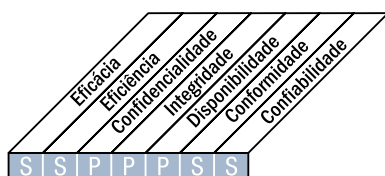
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

P09 Avaliar e Gerenciar os Riscos de TI

Criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.



Controle sobre o seguinte processo de TI:

Avaliar e gerenciar os riscos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

analisar e comunicar os riscos de TI e seus possíveis impactos nos processos e objetivos de negócio

com foco em:

desenvolver uma estrutura de gerenciamento de risco integrada às estruturas corporativa e operacional de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual

é alcançado por:

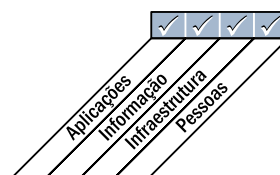
- Garantia de que o gerenciamento de risco esteja completamente integrado aos processos gerenciais, interna e externamente, e seja aplicado de forma consistente
- Realização de avaliações de risco
- Recomendação e comunicação de planos de ação de remediação dos riscos.

e medido por:

- Percentual de objetivos críticos de TI cobertos pela avaliação de risco
- Percentual de riscos críticos de TI identificados que tenham planos de ação desenvolvidos
- Percentual dos planos de ação de gestão de risco aprovados para implementação



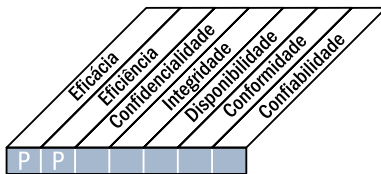
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

P010 Gerenciar Projetos

Estabelecer um programa e uma estrutura de gestão de projeto para o gerenciamento de todos os projetos de TI. Essa estrutura deve assegurar a correta priorização e a coordenação de todos os projetos. A estrutura deve incluir um plano mestre, atribuição de recursos, definição dos resultados a serem entregues, aprovação dos usuários, uma divisão por fases de entrega, garantia da qualidade, um plano de teste formal e uma revisão pós-implementação para assegurar a gestão de risco do projeto e a entrega de valor para o negócio. Esta abordagem reduz o risco de custos inesperados e de cancelamentos de projeto, aperfeiçoa a comunicação, melhora o envolvimento das áreas de negócio e dos usuários finais, assegura o valor e a qualidade dos resultados do projeto e maximiza a contribuição para os programas de investimentos em TI.



Controle sobre o seguinte processo de TI:

Gerenciar Projetos

que satisfaça aos seguintes requisitos do negócio para a TI:

entregar resultados de projetos dentro do tempo, do orçamento e da qualidade acordados

com foco em:

aplicar aos projetos de TI um programa definido e uma abordagem de gestão de projetos que permitam a participação das partes interessadas e a monitoração do andamento e dos riscos do projeto

é alcançado por:

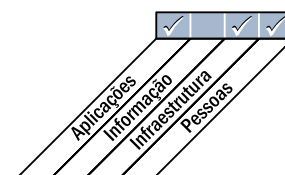
- Definição e implantação de programas, estruturas e abordagens de projeto
- Publicação de diretrizes de gestão de projeto
- Realização de planejamento de projeto para todo o portfólio de projetos

e medido por:

- Percentual de projetos que atendem às expectativas das partes interessadas (prazo, orçamento e escopo – ponderados de acordo com a importância)
- Percentual de projetos que foram revisados após a implementação
- Percentual de projetos que seguem os padrões e as práticas de gerenciamento de projetos



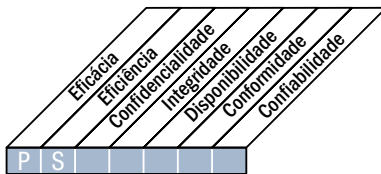
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

AI1 Identificar Soluções Automatizadas

A necessidade de uma nova aplicação ou função requer uma análise prévia à aquisição ou ao desenvolvimento para assegurar que os requisitos de negócio sejam atendidos através de uma abordagem eficaz e eficiente. Este processo contempla a definição das necessidades, considera fontes alternativas, a revisão de viabilidade econômica e tecnológica, a execução das análises de risco e de custo-benefício e a obtenção de uma decisão final por “desenvolver” ou “comprar”. Todos esses passos permitem às organizações minimizar os custos de aquisição e implementação de soluções e permitem ao negócio alcançar seus objetivos.



Controle sobre o seguinte processo de TI:

Identificar Soluções Automatizadas

que satisfaça aos seguintes requisitos do negócio para a TI:

traduzir os requisitos funcionais de negócio e de controle em um projeto eficiente e eficaz de soluções automatizadas

com foco em:

identificar soluções tecnicamente viáveis e com boa relação custo-benefício

é alcançado por:

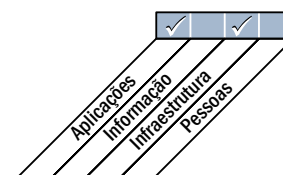
- Definição dos requisitos técnicos e de negócio
- Realização de estudos de viabilidade conforme definido nos padrões de desenvolvimento
- Aprovação (ou rejeição) de requisitos e resultados de estudos de viabilidade

e medido por:

- Quantidade de projetos nos quais os benefícios esperados não foram alcançados devido a premissas incorretas de viabilidade
- Percentual de estudos de viabilidade aceitos pelos respectivos proprietários de processos de negócios
- Percentual de usuários satisfeitos com as funcionalidades entregues



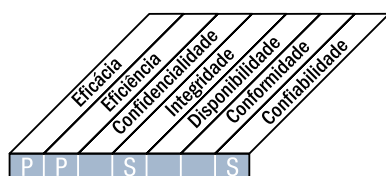
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

AI2 Adquirir e Manter Software Aplicativo

As aplicações devem ser disponibilizadas em alinhamento com os requisitos do negócio. Este processo contempla o projeto das aplicações, a inclusão de controles e requisitos de segurança apropriados, o desenvolvimento e a configuração de acordo com padrões. Isso permite às organizações apoiarem de forma adequada as operações do negócio com as aplicações corretas.



Controle sobre o seguinte processo de TI:

Adquirir e Manter Software Aplicativo

que satisfaça aos seguintes requisitos do negócio para a TI:

tornar disponíveis as aplicações em alinhamento com os requisitos do negócio,
no prazo desejado e com um custo razoável

com foco em:

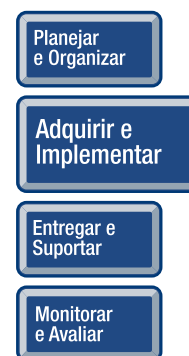
assegurar a existência de um processo de desenvolvimento que contemple o cumprimento
de prazos e otimização de custos

é alcançado por:

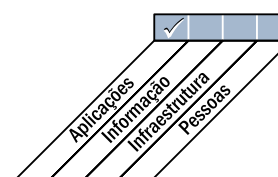
- Tradução dos requisitos de negócio nas especificações de projeto
- Adesão aos padrões de desenvolvimento em todas as modificações
- Segregação entre as atividades de desenvolvimento, teste e operação

e medido por:

- Quantidade de problemas em produção por aplicação que causem períodos perceptíveis de indisponibilidade
- Percentual de usuários satisfeitos com a funcionalidade oferecida



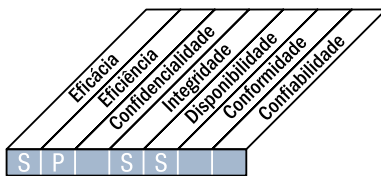
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

AI3 Adquirir e Manter Infraestrutura de Tecnologia

As organizações devem ter processos de aquisição, implementação e atualização da infraestrutura de tecnologia. Isso requer uma abordagem planejada de aquisição, manutenção e proteção da infraestrutura em alinhamento com as estratégias tecnológicas acordadas e o fornecimento de ambientes de desenvolvimento e teste. Isso assegura um apoio tecnológico contínuo às aplicações de negócio.



Controle sobre o seguinte processo de TI:

Adquirir e manter infraestrutura tecnológica

que satisfaça aos seguintes requisitos do negócio para a TI:

adquirir e manter uma infraestrutura de TI integrada e padronizada

com foco em:

Disponibilizar plataformas apropriadas às aplicações de negócio em alinhamento com a arquitetura de TI definida e os padrões tecnológicos

é alcançado por:

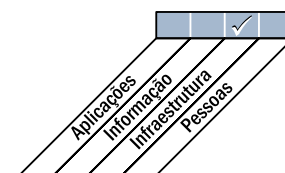
- Preparação de um plano de aquisição tecnológica alinhado com o plano de infraestrutura tecnológica
- Planejamento da manutenção da infraestrutura
- Implementação de controles internos, medidas de segurança e de auditoria

e medido por:

- Percentual das plataformas que não estejam alinhadas com os padrões definidos de tecnologia e arquitetura de TI
- Quantidade de processos críticos de negócio sustentados por infraestrutura obsoleta (ou próxima da obsolescência)
- Quantidade de componentes de infraestrutura que não contam mais com suporte (ou que tendem a não ter suporte num futuro próximo)



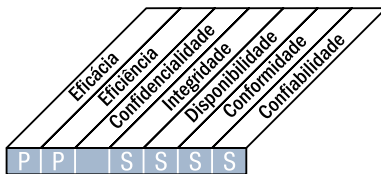
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

AI4 Habilitar Operação e Uso

Conhecimento sobre novos sistemas deve estar disponível. Este processo requer a elaboração de documentação e manuais para usuários e para TI e a promoção de treinamentos para assegurar a operação e uso apropriado das aplicações e infraestrutura.



Controle sobre o seguinte processo de TI:

Habilitar operação e uso

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar a satisfação de usuários finais com ofertas de serviços e níveis de serviços e a completa integração das aplicações e soluções tecnológicas aos processos de negócio

com foco em:

fornecer manuais de usuário, manuais operacionais e materiais de treinamento eficazes para transferir o conhecimento necessário a operação e uso bem-sucedido do sistema.

é alcançado por:

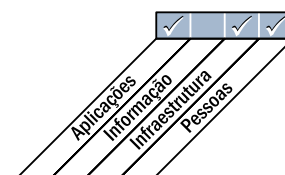
- Desenvolvimento e disponibilização de documentação de transferência de conhecimento
- Comunicação e treinamento de usuários, gestores de negócio, equipes de suporte e equipes de operação
- Produção de materiais de treinamento

e medido por:

- Quantidade de aplicações nas quais os procedimentos de TI estão completamente integrados aos processos de negócio
- Percentual de proprietários de negócio satisfeitos com os treinamentos e material de suporte das aplicações
- Quantidade de aplicações que dispõem de treinamento adequado de suporte operacional e de usuário



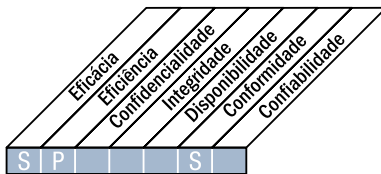
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

AI5 Adquirir Recursos de TI

Recursos de TI, incluindo pessoas, hardware, software e serviços precisam ser adquiridos. Isso requer a definição e a aplicação de procedimentos de aquisição, a seleção de fornecedores, o estabelecimento de arranjos contratuais e a aquisição propriamente dita. Assim assegura-se que a organização tenha todos os recursos de TI necessários a tempo e com boa relação custo-benefício.



Controle sobre o seguinte processo de TI:

Adquirir recursos de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

melhorar o custo-eficiência de TI e sua contribuição para a lucratividade do negócio

com foco em:

adquirir e manter habilidades de TI que respondam à estratégia de entrega e a uma infraestrutura de TI padronizada e integrada, e reduzir o risco de aquisição de recursos de TI

é alcançado por:

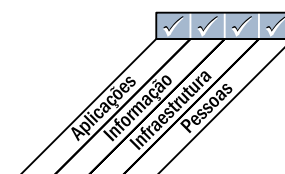
- Obtenção de parecer profissional para aspectos legais e contratuais
- Definição de procedimentos e padrões de aquisição
- Aquisição de hardware, software e serviços requeridos em alinhamento com os procedimentos definidos

e medido por:

- Quantidade de discordâncias relacionadas aos contratos de aquisição
- Custo reduzido de compra
- Percentual das principais partes interessadas satisfeitas com os fornecedores



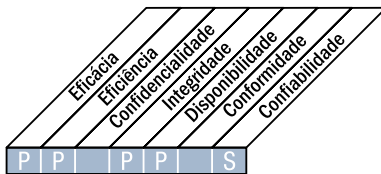
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

AI6 Gerenciar Mudanças

Todas as mudanças, incluindo manutenções e correções de emergência, relacionadas com a infraestrutura e as aplicações no ambiente de produção são formalmente gerenciadas de maneira controlada. As mudanças (incluindo procedimentos, processos, parâmetros de sistemas e de serviço) devem ser registradas, avaliadas e autorizadas antes da implementação e revisadas em seguida, tendo como base os resultados efetivos e planejados. Isso assegura a mitigação de riscos de impactos negativos na estabilidade ou na integridade do ambiente de produção.



Controle sobre o seguinte processo de TI:

Gerenciar Mudanças

que satisfaça aos seguintes requisitos do negócio para a TI:

atender aos requisitos de negócio em alinhamento com a estratégia da organização, reduzindo retrabalho e defeitos na entrega de soluções e serviços

com foco em:

controlar a avaliação de impacto, autorização e implementação de todas as mudanças na infraestrutura, nas aplicações e nas soluções técnicas de TI, minimizar erros devido a especificações de requisitos incompletas e interromper a implementação de mudanças não autorizadas

é alcançado por:

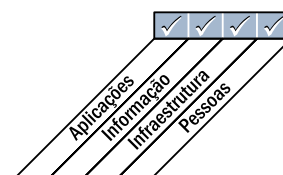
- Definição e comunicação de procedimentos de mudanças, incluindo mudanças emergenciais.
- Avaliação, priorização e autorização de mudanças.
- Acompanhamento de status e apresentação de relatório de mudanças.

e medido por:

- Quantidade de paradas ou erros em dados devido a especificações inadequadas ou avaliações de impacto críticas incompletas
- Retrabalho de infraestrutura ou aplicação causado por especificações de mudança inadequadas
- Percentual de mudanças que seguem o processo formal de controle de mudanças.



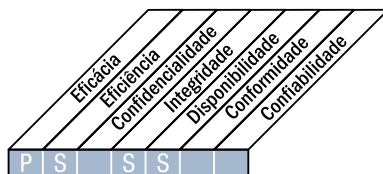
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

AI7 Instalar e Homologar Soluções e Mudanças

Novos sistemas precisam ser colocados em operação uma vez concluído seu desenvolvimento. É necessária a realização de testes apropriados em um ambiente dedicado, com dados de teste relevantes, definição de instruções de implantação e migração, planejamento de liberação e mudanças no ambiente de produção e uma revisão pós-implementação. Isso assegura que os sistemas operacionais estejam alinhados com as expectativas e os resultados acordados.



Controle sobre o seguinte processo de TI:

Instalar e homologar soluções e mudanças

que satisfaça aos seguintes requisitos do negócio para a TI:

sistemas novos ou alterados funcionem sem maiores problemas após a instalação

com foco em:

Testar se as aplicações e as soluções de infraestrutura atendem ao propósito pretendido e estão livres de erros e planejar a implementação e a migração para produção

é alcançado por:

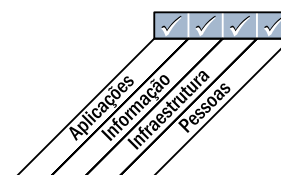
- Estabelecimento de metodologia de teste
- Realização de planejamento de liberação para produção
- Avaliação e aprovação dos resultados de testes pelos responsáveis pelo gerenciamento de negócio
- Realização de revisões após a implementação

e medido por:

- Tempo de indisponibilidade da aplicação ou quantidade de correções de dados devido a testes inadequados
- Percentual de sistemas que na avaliação pós-implementação alcança os benefícios planejados originalmente
- Percentual de projetos que tenham plano de testes documentado e aprovado



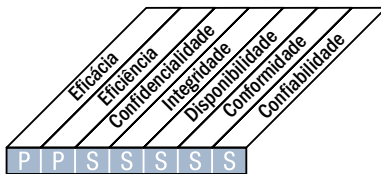
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

DS1 Definir e Gerenciar Níveis de Serviço

A comunicação eficaz entre a Direção de TI e os clientes de negócio sobre os serviços necessários é possibilitada por um acordo definido e documentado que aborda os serviços de TI e os níveis de serviço esperados. Este processo também inclui monitoramento e relatório oportuno às partes interessadas quanto ao atendimento dos níveis de serviço. Este processo permite o alinhamento entre os serviços de TI e os respectivos requisitos do negócio.



Controle sobre o seguinte processo de TI:

Definir e gerenciar níveis de serviço

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar o alinhamento dos principais serviços de TI com a estratégia de negócio

com foco em:

identificar os requisitos de serviço, acordar os níveis de serviço e monitorar o atendimento desses níveis de serviço

é alcançado por:

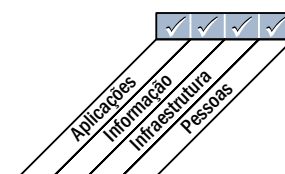
- Formalização de acordos de níveis de serviços internos e externos alinhados com os requisitos e com a capacidade de entrega.
- Reporte do atendimento aos níveis de serviços acordados (reuniões e relatórios)
- Identificação e comunicação de requisitos de serviços novos e atualizados para o planejamento estratégico

e medido por:

- Percentual das partes interessadas que entendem que os níveis de entrega de serviço estão de acordo com os níveis acordados
- Quantidade de serviços prestados inexistentes no catálogo
- Quantidade anual de reuniões formais de análise crítica de acordo de nível de serviço (SLA) com os representantes do negócio.



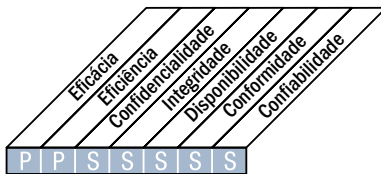
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

DS2 Gerenciar Serviços Terceirizados

A necessidade de assegurar que os serviços prestados por fornecedores satisfaçam aos requisitos do negócio requer um processo efetivo de gestão da terceirização. Esse processo é realizado definindo-se claramente os papéis, responsabilidades e expectativas nos acordos de terceirização bem como revisando e monitorando tais acordos quanto à efetividade e à conformidade. A gestão eficaz dos serviços terceirizados minimiza os riscos de negócio associados aos fornecedores que não cumprem seu papel.



Controle sobre o seguinte processo de TI:

Gerenciar os serviços terceirizados

que satisfaça aos seguintes requisitos do negócio para a TI:

fornecer serviços terceirizados satisfatórios e transparentes do ponto de vista de benefícios, custos e riscos

com foco em:

estabelecer relacionamentos e responsabilidades bilaterais com prestadores de serviço terceirizados qualificados e monitorar a entrega dos serviços para verificar e assegurar o cumprimento dos acordos

é alcançado por:

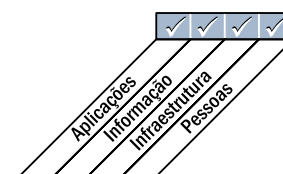
- Identificação e categorização dos prestadores de serviços
- Identificação e redução dos riscos associados ao fornecedor
- Monitoração e medição do desempenho do fornecedor

e medido por:

- Quantidade de reclamações de usuários devido aos serviços contratados
- Percentual de grandes fornecedores que atendam claramente aos requisitos e níveis de serviço definidos
- Percentual de grandes fornecedores sujeitos a monitoramento



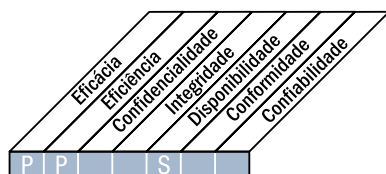
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

DS3 Gerenciar o Desempenho e a Capacidade

A necessidade de gerenciar o desempenho e a capacidade dos recursos de TI requer um processo que realize análises críticas periódicas do desempenho e da capacidade atuais dos recursos de TI. Esse processo inclui a previsão de necessidades futuras com base em requisitos de carga de trabalho, armazenamento e contingência. Esse processo assegura que os recursos de informação que suportam os requisitos do negócio estejam sempre disponíveis.



Controle sobre o seguinte processo de TI:

Gerenciar o desempenho e a capacidade

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar o desempenho da infraestrutura, dos recursos e das capacidades de TI em resposta às necessidades do negócio

com foco em:

atender aos requisitos de tempo de resposta dos diversos acordos de nível de serviço, minimizar o período de indisponibilidade e proporcionar melhorias contínuas no desempenho e na capacidade de TI através de monitoramento e medição

é alcançado por:

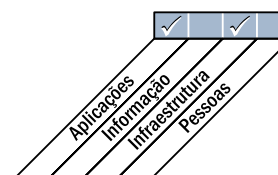
- Planejamento e fornecimento de capacidade e disponibilidade dos sistemas
- Monitoração e informe do desempenho dos sistemas
- Modelagem e previsão do desempenho dos sistemas

e medido por:

- Quantidade de horas perdidas pelo usuário por mês devido ao planejamento insuficiente da capacidade
- Percentual de picos onde a utilização desejada é excedida
- Percentual de tempo de resposta em que os SLAs não são alcançados



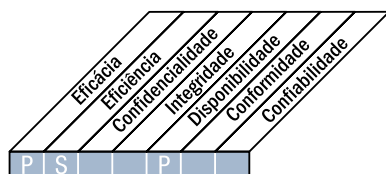
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

DS4 Assegurar a Continuidade dos Serviços

Prover a continuidade dos serviços de TI requer o desenvolvimento, manutenção e teste de um plano de continuidade de TI, armazenamento de cópias de segurança (*backup*) em instalações remotas (*offsite*) e realizar treinamentos periódicos do plano de continuidade. Um processo eficaz de continuidade de serviços minimiza a probabilidade e o impacto de uma interrupção de um serviço chave de TI nas funções e processos críticos de negócio.



Controle sobre o seguinte processo de TI:

Assegurar a continuidade dos serviços

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar um impacto mínimo nos negócios no caso de uma interrupção dos serviços de TI

com foco em:

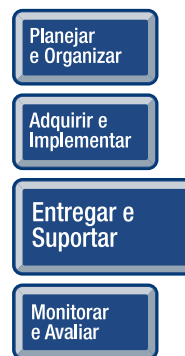
incorporar a capacidade de recuperação em soluções automatizadas e desenvolver, manter e testar os planos de continuidade

é alcançado por:

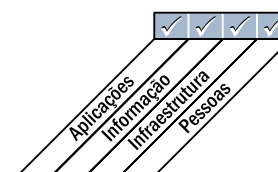
- Desenvolvimento, manutenção e melhoria da contingência de TI
- Treinamento e teste de planos de contingência de TI
- Armazenamento em locais remotos (*offsite*) de cópias dos dados e dos planos de contingência

e medido por:

- Quantidade de horas perdidas por usuários por mês devido inoperância de sistema não planejada
- Quantidade de processos críticos de negócio dependentes da TI e não contemplados no plano de continuidade de TI



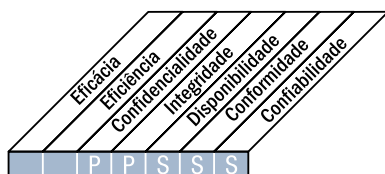
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS5 Garantir a Segurança dos Sistemas

Para manter a integridade da informação e proteger os ativos de TI, é necessário implementar um processo de gestão de segurança. Esse processo inclui o estabelecimento e a manutenção de papéis, responsabilidades, políticas, padrões e procedimentos de segurança de TI. A gestão de segurança inclui o monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança. A gestão eficaz de segurança protege todos os ativos de TI e minimiza o impacto sobre os negócios de vulnerabilidades e incidentes de segurança.



Controle sobre o seguinte processo de TI:

Garantir a segurança dos sistemas

que satisfaça aos seguintes requisitos do negócio para a TI:

manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança

com foco em:

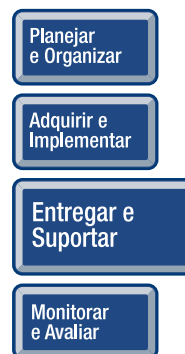
definir políticas, procedimentos e padrões de segurança de TI e monitorar, detectar, reportar e solucionar vulnerabilidades e incidentes de segurança

é alcançado por:

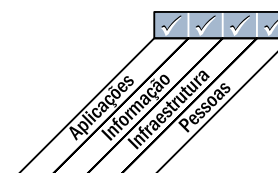
- Entendimento dos requisitos, vulnerabilidades e ameaças de segurança
- Gerenciamento padronizado das identidades e autorizações de usuários
- Testes periódicos de segurança

e medido por:

- Quantidade de incidentes que prejudicam a reputação pública da corporação
- Quantidade de sistemas em que os requisitos de segurança não são atendidos
- Quantidade de violações na segregação de funções



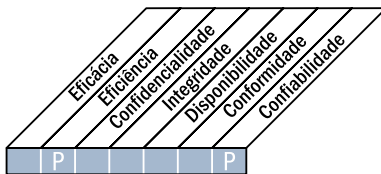
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS6 Identificar e Alocar Custos

A necessidade de um sistema justo e equitativo de alocação de custo de TI para o negócio requer avaliação precisa dos custos de TI e acordo com os usuários do negócio sobre uma alocação razoável. Este processo contempla a construção e a operação de um sistema para capturar, alocar e reportar os custos de TI aos usuários dos serviços. Um sistema de alocação justo permite à empresa tomar decisões mais embasadas sobre o uso dos serviços.



Controle sobre o seguinte processo de TI:

Identificar e alocar custos

que satisfaça aos seguintes requisitos do negócio para a TI:

prover transparência e entendimento dos custos de TI e melhoria da relação custo-benefício através do uso bem informado dos serviços de TI

com foco em:

coleta completa e precisa dos custos de TI, um sistema de alocação justo aceito pelos usuários do negócio e um sistema de reporte oportuno do uso da TI e dos custos alocados

é alcançado por:

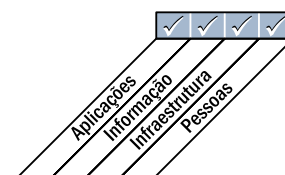
- Alinhamento dos valores cobrados à qualidade e quantidade dos serviços fornecidos
- Construção e concordância de um modelo de custo completo
- Implementação de um sistema de cobrança de valores conforme a política acordada com antecedência

e medido por:

- Percentual de faturas de serviços de TI aceitas/pagas pelo gestor de negócio
- Percentual de variação entre orçamentos, previsões e custos reais
- Percentual dos custos gerais de TI que são alocados de acordo com os modelos de custo combinados



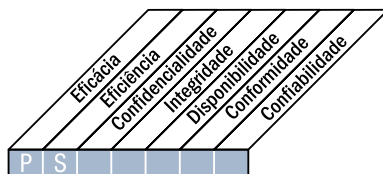
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS7 Educar e Treinar os Usuários

A educação efetiva de todos os usuários de sistemas de TI, inclusive daqueles dentro da própria TI, requer a identificação das necessidades de treinamento de cada grupo de usuário. Como complemento à identificação dessas necessidades, esse processo compreende a definição e a execução de uma estratégia eficaz de treinamento e medição dos resultados. Um programa de treinamento eficaz aumenta o uso efetivo da tecnologia através da redução dos erros de usuário, aumento da produtividade e aumento da conformidade com os controles principais (como as medidas de segurança do usuário).



Controle sobre o seguinte processo de TI:

Educar e treinar os usuários

que satisfaça aos seguintes requisitos do negócio para a TI:

uso efetivo e eficiente das aplicações e soluções tecnológicas, e conformidade do usuário com as políticas e os procedimentos

com foco em:

entender claramente as necessidades do usuário em termos de treinamento em TI e executar uma estratégia eficaz de treinamento e medição dos resultados

é alcançado por:

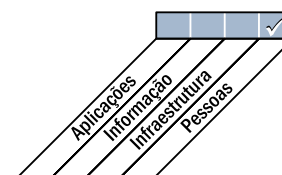
- Estabelecimento de uma grade de treinamento
- Organização de treinamento
- Disponibilização de treinamento
- Monitoramento e relatório da eficácia do treinamento

e medido por:

- Quantidade de chamadas ao centro de atendimento devido à falta de treinamento dos usuários
- Percentual de partes interessadas satisfeitas com o treinamento recebido
- Tempo entre a identificação da necessidade de treinamento e a respectiva realização



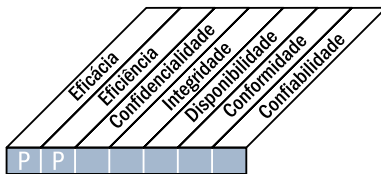
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS8 Gerenciar a Central de Serviço e os Incidentes

A resposta efetiva e em tempo adequado a dúvidas e problemas dos usuários de TI requer uma central de serviço (*service desk*) e processos de gerenciamento de incidentes bem projetados e implementados. Esse processo inclui a implementação de uma central de serviços capacitada para o tratamento de incidentes, incluindo registro, encaminhamento, análise de tendências, análise de causa-raiz e resolução. Os benefícios ao negócio incluem aumento de produtividade por meio de resolução rápida dos chamados dos usuários. Complementarmente, as áreas de negócio podem tratar as causas-raiz (como treinamento deficiente de usuário), através de relatórios efetivos.



Controle sobre o seguinte processo de TI:

Gerenciar a central de serviço e os incidentes

que satisfaça aos seguintes requisitos do negócio para a TI:

permitir o uso eficaz dos sistemas de TI através de análise e resolução de consultas, solicitações e incidentes

com foco em:

prover uma central de serviços profissional com respostas rápidas, procedimentos claros de escalonamento, análise de tendências e resolução

é alcançado por:

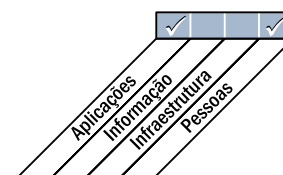
- Instalação e operação de uma central de serviços
- Monitoração e registro das tendências
- Definição clara de critérios e procedimentos de escalonamento

e medido por:

- Satisfação do usuário com o primeiro nível de atendimento
- Percentual de incidentes resolvidos no tempo estipulado/aceitável
- Índice de desistência dos chamados



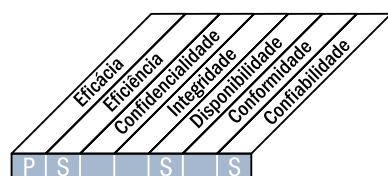
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS9 Gerenciar a Configuração

Assegurar a integridade das configurações de *hardware* e *software* requer o estabelecimento e a manutenção de um repositório de configuração preciso e completo. Esse processo inclui a coleta inicial das informações de configuração, o estabelecimento de um perfil básico, a verificação e a auditoria das informações de configuração e a atualização do repositório de configuração conforme necessário. Um gerenciamento de configuração eficaz facilita uma maior disponibilidade do sistema, minimiza as questões de produção e soluciona problemas com mais rapidez.



Controle sobre o seguinte processo de TI:

Gerenciar a configuração

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar a infraestrutura, os recursos e as capacidades de TI e responder pelos ativos de TI

com foco em:

estabelecer e manter um repositório preciso e completo de atributos e perfis mínimos de configuração de ativos e comparar com a configuração atual dos ativos

é alcançado por:

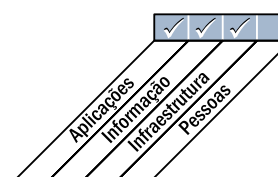
- Estabelecimento de um repositório central de todos os itens de configuração
- Identificação e manutenção dos itens de configuração
- Revisão da integridade dos dados de configuração

e medido por:

- Quantidade de problemas de conformidade de negócio causados pela configuração imprópria dos recursos
- Quantidade de desvios identificados entre o repositório de configuração e as configurações reais dos ativos
- Percentual de licenças adquiridas e não contabilizadas no repositório



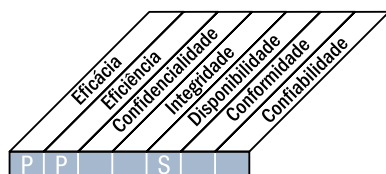
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS10 Gerenciar Problemas

O efetivo gerenciamento de problemas requer identificação e classificação dos problemas, análise de causas-raiz e respectiva resolução. O processo de gerenciamento de problemas também contempla a identificação de recomendações para melhoria, manutenção dos registros de problemas e revisão da situação das ações corretivas. Um processo efetivo de gerenciamento de problemas melhora os níveis de serviço, reduz os custos e aumenta a conveniência e a satisfação do cliente.



Controle sobre o seguinte processo de TI:

Gerenciar os problemas

que satisfaça aos seguintes requisitos do negócio para a TI:

assegurar a satisfação dos usuários finais com a oferta de serviços e níveis de serviço, e reduzir a entrega de serviços e soluções com problemas e re-trabalhos

com foco em:

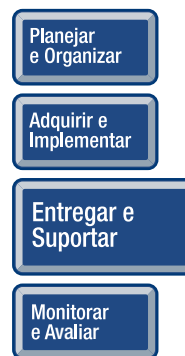
registrar, rastrear e resolver problemas operacionais; investigar a causa-raiz de todos os problemas importantes e definir as soluções para os problemas operacionais identificados.

é alcançado por:

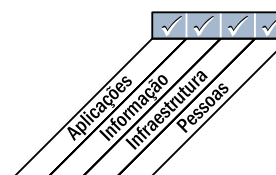
- Realização de análises da causa-raiz do problema reportado
- Análise das tendências
- Propriedade dos problemas e progresso em sua resolução

e medido por:

- Quantidade de problemas recorrentes com impacto sobre os negócios
- Percentual de problemas resolvidos dentro do período de tempo requerido
- Frequência dos reportes ou atualizações de problemas existentes, com base na severidade do problema.



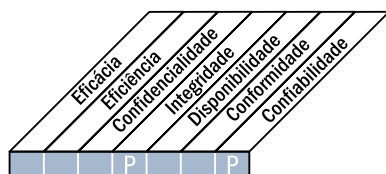
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS11 Gerenciar os Dados

O efetivo gerenciamento de dados requer a identificação dos requisitos de dados. O processo de gerenciamento de dados também contempla o estabelecimento de procedimentos efetivos para controlar a biblioteca de mídia, cópia de segurança (*backup*), recuperação de dados e a dispensa de mídias de forma adequada. O efetivo gerenciamento de dados ajuda a assegurar a qualidade, a rapidez e disponibilidade dos dados de negócio.



Controle sobre o seguinte processo de TI:

Gerenciar os dados

que satisfaça aos seguintes requisitos do negócio para a TI:

otimizar o uso da informação e garantir que a informação esteja disponível quando requisitada

com foco em:

manter a completude, a precisão, a disponibilidade e a proteção dos dados

é alcançado por:

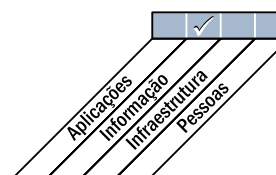
- Realização de cópia de segurança (*backup*) dos dados e testes de restauração
- Gerenciamento de armazenamento local e remoto dos dados (*onsite e offsite*)
- Descarte seguro de dados e equipamentos

e medido por:

- Satisfação do usuário com a disponibilidade dos dados
- Percentual de restaurações de dados bem-sucedidas
- Volume de incidentes nos quais dados confidenciais foram recuperados com sucesso após descarte da mídia.



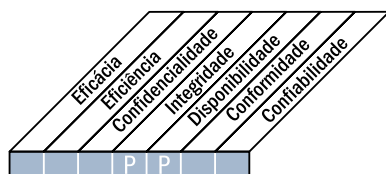
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS12 Gerenciar o Ambiente Físico

A proteção de pessoas e equipamento de informática requer instalações físicas bem planejadas e gerenciadas. O processo de gerenciamento do ambiente físico inclui a definição dos requisitos do local físico, a escolha de instalações apropriadas, o projeto de processos eficazes de monitoramento dos fatores ambientais e o gerenciamento de acessos físicos. O gerenciamento eficaz do ambiente físico reduz as interrupções nos negócios provocadas por danos causados a equipamentos ou pessoas.



Controle sobre o seguinte processo de TI:

Gerenciar o ambiente físico

que satisfaça aos seguintes requisitos do negócio para a TI:

proteger os ativos de TI e os dados do negócio e minimizar o risco de interrupção nos negócios

com foco em:

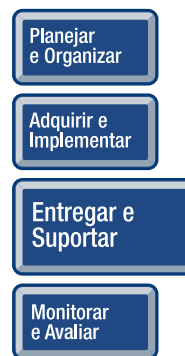
prover e manter um ambiente físico adequado que proteja os recursos de TI contra acesso indevido, danos ou roubo

é alcançado por:

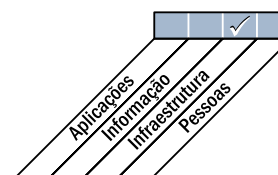
- Implementação de medidas de segurança física
- Seleção e gerenciamento de instalações físicas

e medido por:

- Tempo de indisponibilidade devido a incidentes no ambiente físico
- Quantidade de incidentes causados por falhas ou violação da segurança física
- Frequência das avaliações e revisões de riscos físicos



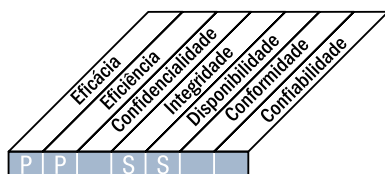
■ Primário ■ Secundário



DESCRIÇÃO DO PROCESSO

DS13 Gerenciar as Operações

O processamento preciso e completo de dados requer um gerenciamento eficaz do processamento de dados e diligente manutenção de *hardware*. Este processo inclui a definição de políticas e procedimentos de operações para o gerenciamento eficaz do processamento agendado, proteção de resultados sigilosos, monitoramento de infraestrutura e manutenção preventiva de *hardware*. O efetivo gerenciamento de operações ajuda a manter a integridade dos dados e reduzir atrasos e custos de operação de TI.



Controle sobre o seguinte processo de TI:

Gerenciar as Operações

que satisfaça aos seguintes requisitos do negócio para a TI:

manter a integridade dos dados e assegurar que a infraestrutura de TI possa resistir e se recuperar de erros e falhas

com foco em:

atingir os níveis de serviço operacionais para o processamento programado de dados, proteção das saídas de dados críticos, monitoramento e manutenção da infraestrutura

é alcançado por:

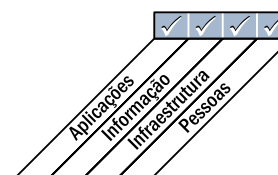
- Operação do ambiente de TI alinhado com os acordos de níveis de serviço e instruções definidas
- Manutenção da infraestrutura de TI

e medido por:

- Quantidade de níveis de serviço impactados por incidentes operacionais
- Quantidade de horas de paradas não programadas causadas por incidentes operacionais
- Percentual de ativos de hardware incluídos na programação de manutenção preventiva



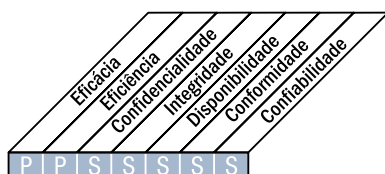
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

ME1 Monitorar e Avaliar o Desempenho de TI

A gestão eficaz de desempenho de TI exige um processo de monitoramento. Esse processo inclui a definição de indicadores de desempenho relevantes, informes de desempenho sistemáticos e oportunos e uma pronta ação em relação aos desvios encontrados. O monitoramento é necessário para assegurar que as atividades corretas estejam sendo feitas e que estejam em alinhamento com as políticas e diretrizes estabelecidas.



Controle sobre o seguinte processo de TI:

Monitorar e avaliar o desempenho de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

transparência e entendimento de custos, benefícios, estratégia, políticas e níveis de serviços de TI, em conformidade com os requisitos de governança

com foco em:

monitorar e entregar relatórios sobre as métricas dos processos de TI e identificar e implementar ações de melhoria de desempenho

é alcançado por:

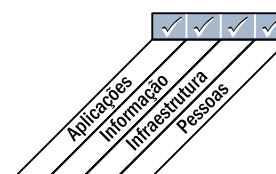
- Agrupamento e tradução dos relatórios de desempenho de processos para relatórios de gestão
- Análise crítica de desempenho frente a metas acordadas e a tomada de ações corretivas necessárias

e medido por:

- Satisfação da Alta Direção e das entidades de governança com os relatórios de desempenho
- Quantidade de ações de melhoria resultantes das atividades de monitoramento
- Percentual de processos críticos monitorados



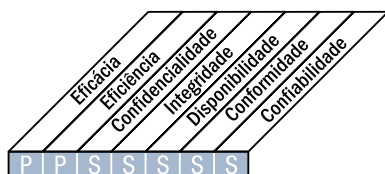
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

ME2 Monitorar e Avaliar os Controles Internos

Estabelecer um programa eficaz de controles internos de TI requer um processo de monitoramento bem definido. Esse processo inclui o monitoramento e reporte das exceções de controle, dos resultados de autoavaliação e avaliação de terceiros. Um benefício importante do monitoramento dos controles internos é assegurar uma operação eficaz e eficiente e a conformidade com as leis e os regulamentos aplicáveis.



Controle sobre o seguinte processo de TI:

Monitorar e avaliar os controles internos

que satisfaça os seguintes requisitos do negócio para a TI:

assegurar que os objetivos de TI sejam atingidos e assegurar a conformidade com as leis e os regulamentos relacionados à TI

com foco em:

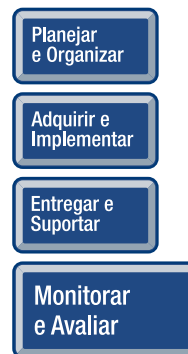
monitorar os processos de controle interno de atividades de TI e identificar ações de melhoria

é alcançado por:

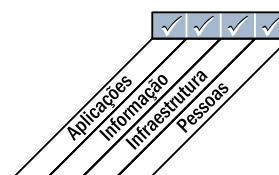
- Definição de um sistema de controles internos integrado na estrutura de processos de TI
- Monitoramento e reporte sobre a eficácia dos controles internos de TI
- Reporte das exceções dos controles internos para que os gestores tomem as medidas necessárias

e medido por:

- Quantidade de falhas críticas nos controles internos
- Quantidade de ações de melhoria dos controles internos
- Quantidade e abrangência das auto-avaliações dos controles internos



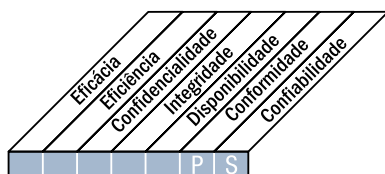
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

ME3 Assegurar a Conformidade com Requisitos Externos

A supervisão eficaz da conformidade requer o estabelecimento de um processo de revisão para assegurar a conformidade com as leis e regulamentações e os requisitos contratuais. Esse processo inclui identificar os requisitos de conformidade, otimizar e avaliar a resposta, assegurar que os requisitos sejam atendidos e integrar os relatórios de conformidade de TI com os das áreas de negócios.



Controle sobre o seguinte processo de TI:

Assegurar a conformidade com requisitos externos

que satisfaça aos seguintes requisitos do negócio para a TI:

estar em conformidade com leis, regulamentações e requisitos contratuais

com foco em:

identificar todas as leis, regulamentações e contratos aplicáveis e o respectivo nível necessário de conformidade de TI e otimizar processos de TI para reduzir o risco de não-conformidade

é alcançado por:

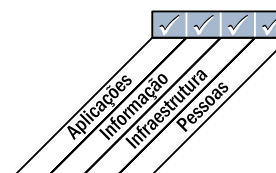
- Identificação dos requisitos legais, regulatórios e contratuais relacionados à TI
- Avaliação do impacto dos requisitos de conformidade
- Monitoramento e geração de relatórios sobre a conformidade com esses requisitos

e medido por:

- Custo da não-conformidade da TI, incluindo multas e penalidades
- Intervalo entre a identificação dos problemas de conformidade externa e sua resolução
- Frequência das revisões de conformidade



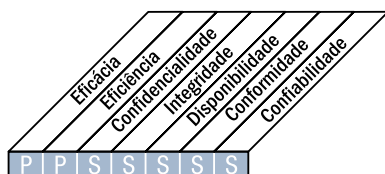
■ Primário ■ Secundário



DESCRIÇÃO DE PROCESSO

ME4 Prover Governança de TI

O estabelecimento de uma efetiva estrutura de governança envolve a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos corporativos em TI estejam alinhados e sejam entregues em conformidade com as estratégias e os objetivos da organização.



Controle sobre o seguinte processo de TI:

Prover Governança de TI

que satisfaça aos seguintes requisitos do negócio para a TI:

integrar a governança de TI aos objetivos de governança corporativa e ter conformidade com leis, regulamentações e contratos

com foco em:

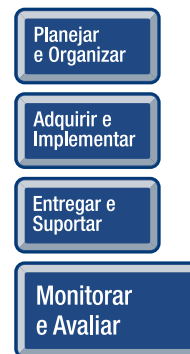
preparar relatórios gerenciais sobre a estratégia, o desempenho e os riscos de TI
e atender aos requisitos de governança em alinhamento com as diretrizes da Alta Direção

é alcançado por:

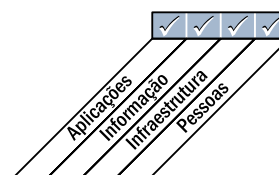
- Estabelecimento de uma estrutura de governança de TI integrada à governança corporativa
- Auditoria independente do status da governança de TI

e medido por:

- Frequência dos relatórios gerenciais sobre TI para as partes interessadas (inclusive maturidade)
- Frequência dos relatórios de TI para a Alta Direção (inclusive maturidade)
- Frequência das revisões independentes da conformidade de TI



■ Primário ■ Secundário



ANEXO IV – Plano de Ações para Implementação da Governança de TI

Objetivo

Obter aceitação e integração dos conceitos do COBIT na organização, incluindo a Auditoria, Operações, Tecnologia e serviços terceirizados.

Objetivos específicos

1. Continuar a prestar serviços essenciais de auditoria e controle, ampliando e adaptando para garantir a cobertura dos processos do COBIT relevantes ao negócio e setor.
2. Assegurar que as necessidades de informação da empresa serão atendidas pelo departamento de tecnologia em conformidade com os critérios de informação definidos no COBIT.
3. Assegurar que atividades de planejamento e organização significastes identificadas no COBIT sejam adotadas pelo departamento de tecnologia da organização.
4. Assegurar que aquisições e implementações significativas identificadas pelo COBIT serão empregados nos serviços prestados pelo departamento de tecnologia e incorporadas no gerenciamento de projetos utilizado pela organização.
5. Assegurar que atividades de entrega e suporte significativas identificadas pelo COBIT serão providas para clientes internos pelo departamento de tecnologia e provedores de serviços terceirizados.
6. Assegurar que os processos de monitoramento significativos identificados pelo COBIT serão empregados pelos departamentos de tecnologia e auditoria.

Abordagem

- Familiarização
- Educação
- Compromisso
- Adaptação
- Implementação

Sequência

- Departamento de Auditoria
- Departamento de Tecnologia
- Prestadores de serviços terceirizados
- Alta Gerência
- Comitês de Auditoria

Processos

1. Distribuir cópias do Sumário Executivo do COBIT e levantamento preliminar com os gerentes principais, provocando análise e reflexões sobre a situação atual da organização.
2. Compilar os resultados da pesquisa e desenvolver uma apresentação de resultados relativos aos conceitos do COBIT.
3. Apresentar aos gerentes das equipes de Operações e Tecnologia.
4. Apresentar aos profissionais das equipes de Operações e Tecnologia.
5. Apresentar aos gerentes de serviços terceirizados e profissionais principais.
6. Auxiliar os principais gerentes no desenvolvimento de planos de ações para a integração de conceitos nos processos de negócios.
7. Apresentar conceitos do COBIT e relatórios de progresso das atividades para a gerência sênior mantendo-os informados e obter apoio.
8. Reestruturar o inventário de auditoria para refletir a orientação a processos do COBIT.
9. Desenvolver ou atualizar os processos de auditoria em consistência com o guia de auditoria do COBIT.
10. Desenvolver oportunidades de aprendizagem do COBIT de acordo com as necessidades organizacionais.
11. Oferecer formação em COBIT quando necessário.
12. Monitorar o progresso dos planos de ações da Tecnologia.
13. Apresentar conceitos do COBIT, progresso e resultados ao Comitê de Auditoria.

Marcos

- Mês 1 - completar pesquisas e planos de ações
- Mês 2 - apresentar o COBIT para gerentes sênior
- Mês 3 - apresentar o COBIT para o comitê de auditoria

ANEXO V – Relação entre processos dos *frameworks* COBIT e ITIL

COBIT		ITIL
Planejar & Organizar	1. Definir um Plano Estratégico de Tecnologia da Informação	Planejar e controlar serviços de TI
	2. Definir a Arquitetura da Informação	Gestão de Segurança
	3. Determinar Direção Tecnológica	Determinar Direção Tecnológica
	4. Definir a Organização da TI e Relacionamentos	Organização de Serviços de TI
	5. Gestão do Investimento em Tecnologia da Informação	Gestão Financeira
	6. Comunicar Objetivos de Gestão e Direcionamentos	
	7. Gestão de Recursos Humanos	
	8. Garantir Conformidade com requisitos externos	
	9. Identificar Riscos	
	10. Gestão de Projetos	
	11. Gestão da Qualidade	Gestão da Qualidade para Serviços de TI
Adquirir & Implementar	1. Identificar Soluções	Gestão de Níveis de Serviços; Gestão de Mudanças; Gestão da Segurança; Gestão de <i>Release</i>
	2. Adquirir e Manter Software Aplicativo	Gestão de Mudanças; Gestão de Disponibilidade
	3. Adquirir e Manter Arquitetura Tecnológica	Gestão de Problemas; Gestão da Segurança; Gestão de Mudanças
	4. Desenvolver e Manter Procedimentos de Tecnologia da Informação	
	5. Instalar e Certificar Sistemas	Gestão da Capacidade; Gestão de Mudanças; Gestão da Segurança

Tabela 6: Relação entre processos dos frameworks COBIT e ITIL, do autor

ANEXO V – Relação entre processos dos *frameworks* COBIT e ITIL

COBIT		ITIL
Entregar & Suportar	1. Definir Níveis de Serviços	Gestão de Níveis de Serviços
	2. Gestão de Serviços Terceirizados	Gestão de Níveis de Serviços
	3. Gestão de Desempenho e Capacidade	Gestão da Capacidade
	4. Garantir Continuidade dos Serviços	Gestão da Disponibilidade; Planejamento de Contingência
	5. Garantir a Segurança de Sistemas	Gestão da Segurança
	6. Identificar e Alocar Custos	Gestão Financeira
	7. Educar e Treinar Usuários	Relacionamento com o Cliente
	8. Assessorar e Aconselhar Clientes de Tecnologia da Informação	Gestão de Incidentes (<i>Service Desk</i>)
	9. Gestão da Configuração	Gestão da Configuração
	10. Gestão de Problemas e Incidentes	Gestão de Problemas
	11. Gestão de Dados	Gestão da Capacidade; Gestão de <i>Release</i> ; Gestão da Disponibilidade; Planejamento de Contingência
	12. Gestão de Instalações	
	13. Gestão de Operações	
Monitorar & Avaliar	1. Monitoramento de Processos	
	2. Obter Garantias Independentes	
	3. Prover Garantias Independente	
	4. Prover Auditoria Independente	

Tabela 6: Relação entre processos do COBIT e ITIL, do autor

ANEXO VI – Relação entre processos dos *frameworks* ISO/IEC 27002 e ITIL

ISO/IEC 27002:2005	ITIL
Controle de Acesso a Sistemas	Gestão da Segurança
Gestão de Computadores e Operações	Gestão da Infra-estrutura de Tecnologia da Informação
Desenvolvimento e Manutenção de Sistemas	Gestão de Aplicativos
Segurança Física e de Ambiente	Gestão da Segurança
Conformidade	Gestão da Segurança
Equipe de Segurança	Gestão da Segurança
Organização da Segurança	Gestão da Segurança
Classificação e Controle de Ativos	Gestão da Configuração
Gestão da Continuidade de Negócios	Gestão da Continuidade de Serviços de Tecnologia da Informação

Tabela 7: Relação entre processos dos frameworks ISO/IEC 27002 e ITIL, do autor