

**ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB
CURSO PÓS GRADUAÇÃO LATU SENSU EM
ENGENHARIA DE SISTEMAS**

MANOEL AUGUSTO CARDOSO DA FONSECA

**AS CERTIFICAÇÕES ISO 9001, 20000 E 27001 COMO VANTAGEM
COMPETITIVA NA GESTÃO DOS SERVIÇOS DE TI**

VILA VELHA - ES

2011

MANOEL AUGUSTO CARDOSO DA FONSECA

**AS CERTIFICAÇÕES ISO 9001, 20000 E 27001 COMO VANTAGEM
COMPETITIVA NA GESTÃO DOS SERVIÇOS DE TI**

Monografia apresentada ao Curso de Pós-Graduação em Engenharia de Sistemas da Escola Superior Aberta do Brasil como requisito para obtenção do título de Especialista em Engenharia de Sistemas, sob orientação do Prof. Mestre Cleyverson Pereira Costa.

VILA VELHA - ES

2011

MANOEL AUGUSTO CARDOSO DA FONSECA

**AS CERTIFICAÇÕES ISO 9001, 20000 E 27001 COMO VANTAGEM
COMPETITIVA NA GESTÃO DOS SERVIÇOS DE TI**

Monografia aprovada em ... de ... de 2011.

Banca Examinadora

VILA VELHA - ES

2011

DEDICATÓRIA

Dedico este trabalho a minha querida esposa Raquel pelo carinho e amor recebidos durante a elaboração do mesmo e nos demais momentos de nossas vidas. Aos meus filhos Gabriela, Roberto e Manoela pelo amor e orgulho recíproco ao longo de nossas vidas. Aos meus pais Leonardo (in memoriam) e Maria pelo amor, apoio, educação e principalmente exemplo que sempre me ofereceram.

AGRADECIMENTO

Ao Prof. Mestre Orientador Marcos Alexandre do Amaral Ramos, pela orientação durante a elaboração do plano de monografia. Ao Prof. Mestre Cleyverson Pereira Costa pelas sábias orientações imprescindíveis durante a produção do meu trabalho. À Fundação Braslight pela colaboração durante a elaboração do Estudo de Caso, em especial ao Diretor Presidente Eng. Márcio Brito Moraes Jardim pela autorização concedida e aos funcionários da Gluck Informática representados pelo seu diretor Carlos Renato de Barros pelas informações técnicas prestadas. Aos meus colegas, amigos e irmãos pelo apoio recebido. A Deus pelas bênçãos recebidas ao longo de minha vida.

“O que eu ouço, eu esqueço. O que eu vejo, eu lembro. O que eu faço, eu entendo” (Confúcio)

RESUMO

Palavras-chave: Certificações ISO 20000 e 27001, Gestão de Serviços de TI

Esta monografia apresenta a evolução da área de Tecnologia da Informação e os frameworks mais adotados em relação à governança de TI, gestão de serviços, gestão da qualidade e gestão da segurança da informação. Foi também abordado a integração entre o framework Cobit de governança de TI e os sistemas de gestão da qualidade, segurança da informação e serviços. A importância da certificação como vantagem competitiva e os principais elementos das normas ISO 9001, ISO 27001 e ISO 20000. Na abordagem de cada uma das normas procurou-se demonstrar os benefícios adquiridos com sua implantação de forma a apresentar na conclusão uma síntese das vantagens oferecidas nas áreas financeira, operacional, de recursos humanos e comercial/institucional pela adoção dos modelos. O estudo de caso aborda a implementação do sistema de gestão da segurança da informação de forma integrada com o da qualidade e os resultados práticos obtidos na Fundação Braslight.

LISTA DE FIGURAS

FIGURA 1 – FUNCIONAMENTO DO COBIT EM RELAÇÃO AOS FRAMEWORKS DE TI	25
FIGURA 2 - COMPONENTES DO COBIT	25
FIGURA 3 - MODELO PDCA APLICADO AOS PROCESSOS DO SGSI	45
FIGURA 4 - NORMAS ISO DE SISTEMAS DE GESTÃO NA ÁREA DE TI	56
FIGURA 5 - RELACIONAMENTO ENTRE GOVERNANÇA DE TI E NORMAS ISO DE SISTEMAS DE GESTÃO EM TI	65

LISTA DE TABELAS

TABELA 1- IMPACTOS GERADOS POR FALHAS NOS SISTEMAS DE INFORMAÇÃO	20
TABELA 2 - MODELO DE MATURIDADE GENÉRICO.....	30
TABELA 3- EVOLUÇÃO DE CERTIFICADOS ISO 9000 NO BRASIL.....	35
TABELA 4 – NUMERO DE EMPRESAS COM CERTIFICAÇÃO ISO 27001	42

SUMÁRIO

INTRODUÇÃO.....	12
OBJETIVO GERAL	13
OBJETIVOS ESPECÍFICOS	13
METODOLOGIA.....	13
CAPITULO 1 – A EVOLUÇÃO DA TI – DO PROCESSAMENTO DE DADOS A TIC (TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO).....	15
1.1. CONSIDERAÇÕES PARCIAIS.....	18
CAPITULO 2 - A GOVERNANÇA EM TI	19
2.1. INTRODUÇÃO A GOVERNANÇA EM TI.....	19
2.2. COBIT – OBJETIVOS DE CONTROLE PARA INFORMAÇÕES E TECNOLOGIAS RELACIONADAS	24
2.3. BENEFÍCIOS E IMPACTOS GERADOS PELA ADOÇÃO DA GOVERNANÇA EM TI DE FORMA INTEGRADA COM OS DEMAIS SISTEMAS DE GESTÃO. ...	30
CAPITULO 3 – O SISTEMA DE GESTÃO DA QUALIDADE APLICADO A TI – A NORMA ISO-9001	34
3.1. O QUE É A ISO?	34
3.2. O SISTEMA DE GESTÃO DA QUALIDADE ISO 9000.....	35
3.3. BENEFÍCIOS OBTIDOS E IMPACTOS GERADOS ATRAVÉS DA IMPLANTAÇÃO E CERTIFICAÇÃO DA TECNOLOGIA DA INFORMAÇÃO NA NORMA ISO 9001:2008	38
3.4. CONSIDERAÇÕES PARCIAIS.....	40
CAPITULO 4 – O SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E SUA IMPORTÂNCIA – AS NORMAS ISO-27001 E ISO-27002.....	41
4.1. HISTÓRICO DAS NORMAS DA FAMÍLIA ISO 27000	41
4.2. O SISTEMA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO	44
4.3. BENEFÍCIOS E IMPACTOS GERADOS PELA ADOÇÃO E CERTIFICAÇÃO DO SISTEMA DE GESTÃO DA SEGURANÇA DE INFORMAÇÃO PELA TECNOLOGIA DA INFORMAÇÃO	52
4.3. CONSIDERAÇÕES PARCIAIS.....	53
CAPITULO 5 – A GESTÃO DE SERVIÇOS DE TI A NORMA ISO-20000 E AS MELHORES PRÁTICAS COM A ITIL	54
5.1. HISTÓRICO DAS NORMAS DA FAMÍLIA ISO 20000	54
5.2. O SISTEMA DE GESTÃO DE SERVIÇOS BASEADO NA NORMA ISO 20000	55
5.3. BENEFÍCIOS OBTIDOS PELA ADOÇÃO E CERTIFICAÇÃO DO SISTEMA DE GESTÃO DE SERVIÇOS EM TI.....	60
5.4. CONSIDERAÇÕES PARCIAIS.....	61
CAPITULO 6 – ESTUDO DE CASO A IMPLANTAÇÃO DO SISTEMA DE GESTÃO	

DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ISO 27001 NA BRASLIGHT	62
6.1. CONSIDERAÇÕES PARCIAIS	64
CONCLUSÃO	65

INTRODUÇÃO

Sistema de gestão refere-se a tudo o que a organização faz para gerir suas atividades e seus processos. As normas de sistema de gestão fornecem à organização um modelo a ser seguido para preparar, implementar e operar seu sistema de gestão. Este modelo incorpora as melhores práticas já adotadas no mercado com sucesso. Trata-se da gestão de forma sistêmica e a busca da melhoria contínua.

Na área de Tecnologia da informação as normas das séries ISO 9000, ISO 20000 e 27001 definem os Sistemas de Gestão da Qualidade, Gestão de Serviços e Segurança da Informação respectivamente. Procurou-se demonstrar que a adoção das mesmas tem oferecido vantagem competitiva, em relação ao mercado, às empresas que baseiam seus sistemas de gestão nestas normas. Elas permitem a uma organização demonstrar aos seus clientes e investidores que opera com integridade e segurança, e que promove uma cultura de melhoramento contínuo da qualidade no âmbito da Gestão de Serviços de TI.

Os profissionais de Engenharia de Sistemas e Gerência de Projetos, cada vez mais, prestam serviços para organizações com preocupações quanto a conformidade normativa. Neste sentido tanto a produção de software quanto a gestão de projetos e pessoas deve estar relacionada com os processos de qualidade, segurança da informação e gerência de serviços. A TI passa a estar alinhada com os objetivos estratégicos da organização e portanto precisa demonstrar que suas operações e produtos gerados tem integridade e segurança. A Governança em TI passa a ser adotada pelas organizações em larga escala.

Esta monografia pretende demonstrar a importância e as vantagens obtidas com a adoção da governança em TI e de sistemas de gestão da qualidade, de serviços e segurança da informação baseados nas normas das famílias ISO 9000, ISO 20000 e 27000.

O que é necessário para a implantação destas normas pelas empresas e quais os benefícios de sua adoção ? Pretende-se responder estas questões: descrevendo a

evolução da tecnologia da informação e das normas relativas a Governança e Gestão de TI, fornecendo uma perspectiva geral das mesmas e debatendo os impactos e ações a serem adotadas para a implementação das mesmas.

As certificações iso 9001, 20000 e 27001 oferecem diversas vantagens competitivas para empresas que as adotam na gestão dos serviços de ti em relação as que não possuem modelos de sistemas de gestão, o trabalho procurou apresentar estas vantagens e os benefícios gerados pelas mesmas através de fundamentação teórica e um estudo de caso. Procurou-se atingir os seguintes objetivos:

OBJETIVO GERAL

Analisar as vantagens competitivas obtidas por uma organização através da adoção dos sistemas de gestão em qualidade, serviços e segurança da informação com certificação nas normas ISO 9000, ISO 20000 e 27001 em relação às empresas que não cumprem estas normas.

OBJETIVOS ESPECÍFICOS

1. Estabelecer uma análise quanto ao reconhecimento internacional de mercado relativo à certificação nas normas ISO 9000, ISO 20000 e ISO 27001;
2. Analisar os benefícios obtidos com a necessidade de melhoria contínua para a conformidade com as normas;
3. Analisar o valor agregado com a adoção das melhores práticas na Gestão de Serviços e Segurança da Informação.
4. Analisar as vantagens de integração entre as normas de gestão de serviços e segurança da informação com a de gestão da qualidade.
5. Analisar a importância da adoção da Governança Corporativa e objetivos de controle como forma de monitoramento da eficácia dos sistemas de gestão.

METODOLOGIA

A pesquisa adotou a forma explicativa e exploratória. Foram utilizados como apoio os seguintes meios: bibliografia técnica, normas de sistemas de gestão, pesquisa na internet, literaturas científicas, trabalhos acadêmicos, artigos e um estudo de caso. Primeiramente será abordada a evolução da TI (Tecnologia da Informação) e a necessidade de adoção das melhores práticas para o atingimento da Governança em TI, em especial com o foco no modelo Cobit. A seguir serão apresentadas as principais normas orientadoras dos sistemas de gestão da TI e sua integração, concluindo com uma análise das vantagens competitivas e benefícios profissionais adquiridos através de sua implementação e certificação. Em todos os capítulos procura-se apresentar os benefícios da adoção da norma abordada e seus impactos, de forma a apresentar as características congruentes de todas as normas e que estabelecem as vantagens competitivas para quem as adota. O estudo de caso da Fundação Braslight sediada no Rio de Janeiro tem por objetivo apresentar na prática os resultados mensuráveis pela implantação de dois dos sistemas de gestão apresentados, ISO 27001 de forma integrada com a ISO 9001..

CAPITULO 1 – A EVOLUÇÃO DA TI – DO PROCESSAMENTO DE DADOS A TIC (TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO)

O Século XX caracterizou-se pela impressionante evolução dos computadores e suas aplicações. Na década de 60 surgiram as primeiras aplicações comerciais, cujo desenvolvimento na década de 50 restringia-se a aplicações governamentais como apuração do censo e processamento de impostos. Esta década caracterizou-se por: poucas opções tecnológicas (software e equipamentos), linguagens e processos de programação trabalhosos, automação de rotinas manuais, escassez de mão-de-obra e inexistência de metodologias de desenvolvimento.

As décadas de 70 e 80 caracterizaram-se pela expansão das aplicações comerciais, aumentando o impacto dos sistemas nas empresas, passando os profissionais de informática a considerar: conceitos de desenvolvimento organizacional, processo decisório, interface homem-máquina, relacionamento com o usuário e preocupação com ergonomia. Os recursos computacionais passam a apoiar diretamente os negócios. Surge a terceirização do processamento de dados com a criação de grandes bureaus de prestação de serviços. O ambiente externo das empresas começa a mudar com a revolução das comunicações (PACHECO apud REINHARD, 1996).

Oriunda de uma evolução da rede de comunicações militar ARPANET, desenvolvida em função da Guerra Fria, surge na década de 80 a Internet, sendo que nos anos seguintes à sua popularização, seus usuários preocupavam-se com a circulação de textos, uma vez que seu principal objetivo era o intercâmbio entre pesquisadores e universidades. Os microcomputadores popularizaram-se nesta década e iniciou-se um processo de descentralização da utilização da informática, difundindo-se esta nas organizações de qualquer porte. Em 1992 foi criado o primeiro navegador de internet, o Mosaic, que dispunha de interface mais amigável e disponibilizava navegação por links e de imagens. E assim a internet foi se desenvolvendo e se aprimorando. A universalização das telecomunicações e do acesso aos microcomputadores muda de vez o tipo de utilização dos computadores. O termo Processamento de Dados (PD) é definitivamente substituído por Tecnologia da

Informação (TI).

O final do século XX e o início do século XXI têm a TI como centro da estratégia empresarial. A sociedade da informação tem o conhecimento como fonte de geração de valor. A utilização dos computadores pessoais e as redes corporativas ocasionam uma mudança de paradigma. A informação passa a ser considerada um ativo importante das organizações uma vez que se torna uma das principais fontes de geração de valor e como tal aumenta a preocupação com sua proteção. Com estas mudanças nas tecnologias entramos na era da necessidade de integração e reestruturação dos negócios, com a necessidade de intercâmbio entre os sistemas legados e as tecnologias emergentes. A convergência das tecnologias afetam todas as áreas de negócio. O termo TI se transforma em TIC (Tecnologias da Informação e Comunicação) afinal temos de designar o conjunto de recursos tecnológicos, de telecomunicações e computacionais para geração, disponibilização e uso da informação. (PACHECO apud DANIELS, 1996).

A TIC não se restringe a equipamentos (hardware), programas (software), infraestrutura e telecomunicações e como estes recursos estão organizados. A importância adquirida pela TIC determinou o desenvolvimento de sistemas de gestão e planejamento de informática, novas tecnologias de desenvolvimento de sistemas cujo principal foco é a produtividade e interoperabilidade, tarefas de suporte e ensino a distância. Tudo isto se insere dentro do contexto TIC.

Diante deste processo contínuo de evolução, nos dias atuais deve-se destacar dois aspectos relativos a TIC. A evolução da Engenharia de Software, com relevância para novas arquiteturas e tecnologias, como a Arquitetura Orientada a Serviços (SOA), as Tecnologias Ágeis, os Padrões de Projeto e os Web Services. Torna-se relevante neste contexto a adoção da Governança de TI através da implantação de sistemas de gestão com orientação a processos e melhoria contínua como: ITIL, Cobit, Norma ISO 27001 e ISO 20000.

A “Era do Processamento de Dados” onde a informática era mera ferramenta do negócio evoluiu para a “Era da Informação” onde a TIC precisa que seus objetivos estejam alinhados com os da organização como forma de gerar valor.

Os profissionais de engenharia de sistemas e gerência de projetos passam a focar o resultado de suas atividades na agregação de valor ao negócio. Todo o planejamento da área de TIC deve estar de acordo com o planejamento estratégico da organização a que pertence. Processos como gestão de portfólio, gestão de capacidade, gestão de liberação, gestão da segurança da informação e gestão de aquisições são sistematizados e incorporados ao dia a dia da TI, afinal tudo relativo a área de TI deve estar alinhado ao planejamento estratégico da organização. A evolução nos sistemas de gerenciamento da informação e no perfil do profissional da área consolidou a TI como importante ferramenta de gestão, No entender de Rezende (2002, p 2):

“Para atingir a qualidade, produtividade e efetividade nas atividades relacionadas a sistemas empresariais e à TI, que são requeridas pelo mercado de trabalho, há necessidade de um perfil profissional que contemple o domínio das habilidades técnica, de negócio e comportamental. **As habilidades técnicas** são as adquiridas ao longo da formação técnica do profissional, em cursos acadêmicos e em outros complementares. Destacam-se: metodologias, técnicas, ferramentas tecnológicas, linguagens de programação, etc. **As habilidades de negócio** são as adquiridas ao longo do exercício profissional, no desenvolvimento de soluções para as empresas. Destacam-se: negócios em questão, funções empresariais, funções da administração, processos, procedimentos, idiomas, etc. **As habilidades comportamentais** ou humanas são as adquiridas ao longo da vida, ou seja, na educação e nos relacionamentos humanos e corporativos. Destacam-se: proação (iniciativa, execução e conclusão), criatividade, comunicação e expressão, relacionamento pessoal, espírito de equipe e/ou administração participativa, planejamento pessoal, organização, concentração, atenção, disponibilidade, responsabilidade, etc.”

A adoção de sistemas de gestão baseados em processos, tem como um de seus objetivos a padronização das atividades dependentes das habilidades de negócio e a adoção das melhores práticas já comprovadas.

Nos próximos capítulos serão detalhados os principais sistemas de gestão e governança em TI e seus processos, inicialmente fazendo um apanhado dos principais frameworks do mercado e a seguir focando na implantação de sistemas de gestão da segurança da informação e de serviços de TI, baseados nas normas ISO das famílias 9000, 27000 e 20000.

Será demonstrado que os modelos de sistemas de gestão de qualidade, serviços de TI e segurança da informação definidos pelas normas ISO são complementares e

perfeitamente integráveis. O framework de governança de TI Cobit, também é complementar aos sistemas de gestão e sua adoção confia métodos e métricas para avaliação e auditoria dos sistemas de gestão.

A evolução da TI atingiu tal estágio que independente do porte de empresa a adoção de melhores práticas de gestão tornou-se indispensável e a utilização destes sistemas pelos profissionais de TI indispensável.

1.1. CONSIDERAÇÕES PARCIAIS

A TI continua em constante evolução, fala-se agora em convergência digital, que nada mais é do que a integração de mídias que se convergem para interagir em um único ambiente.

Na medida em que a evolução da TI, transforma a sociedade, cresce a importância de termos todos os processos de tratamento da informação definidos e gerenciados quantitativamente. Gerenciar quantitativamente a performance de um processo é estabelecer as métricas de qualidade e desempenho e acompanhar a execução do processo em relação a estas métricas.

Todos os modelos de sistema de gestão adotados, preocupam-se com a melhoria contínua e portanto requerem o estabelecimento de métricas em todos os processos das diversas áreas do sistema de gestão. Afinal: “o que não é medido não pode ser gerenciado”, pois para termos um alinhamento entre os objetivos do negócio e os da área de TI, necessitamos realizar um acompanhamento através de indicadores de desempenho. A adoção de um sistema de gestão certificado assegura que há uma preocupação com a melhoria contínua e que o desempenho do sistema é monitorado continuamente.

CAPITULO 2 - A GOVERNANÇA EM TI

A área mais crítica da Governança Corporativa é a Governança em TI pois a dependência forte do negócio em relação à TI é característica da maioria das empresas nos dias de hoje (SANTOS – 2010). Como os sistemas de gestão estão diretamente relacionados à governança, é importante dar-se uma visão sobre esta.

2.1. INTRODUÇÃO A GOVERNANÇA EM TI

A expressão “governança corporativa” deriva do inglês *“corporate governance”* significando o sistema pelo qual os acionistas de uma empresa “governam” ou seja, tomam conta, de sua empresa. Em resumo: é o conjunto de processos, costumes, políticas, leis, regulamentos e instituições que regulam a maneira como uma empresa é dirigida, administrada ou controlada.

O termo inclui também o estudo sobre as relações entre os diversos atores envolvidos (os *stakeholders*) e os objetivos pelos quais a empresa se orienta. Estes tipicamente são: os acionistas, a alta administração e o conselho de administração. Outros participantes da governança corporativa incluem os funcionários, fornecedores, clientes, bancos e outros credores, instituições reguladoras (como a CVM, o Banco Central, etc.) e a comunidade em geral.

O grande interesse pelo tema inicialmente se deu em função das iniciativas de conformidade na governança corporativa, com a lei Sarbanes-Oxley nos Estados Unidos e o acordo de Basileia II na Europa.. Estas iniciativas se deram principalmente devido aos espetaculares colapsos de grandes corporações norte-americanas como a Enron Corporation, Global Crossing, Tyco Internacional e Worldcom.

No Brasil, em 2001, foi reformulada a Lei das Sociedades Anônimas e, em 2002, a Comissão de Valores Mobiliários (CVM) lançou sua cartilha sobre o tema Governança. Documento focado nos administradores, conselheiros, acionistas e

auditores independentes. Esta Cartilha visa orientar sobre as questões que afetam o relacionamento entre os já citados. Muito em função do alinhamento entre o planejamento estratégico das organizações e o da Tecnologia da Informação, agregando-se a isto, a necessidade de conformidade com as normas internacionais, a Governança em TI acompanhou o crescimento de importância da Governança Corporativa.

A Governança em TI pode ser considerada um subconjunto da governança corporativa abrangendo os sistemas e processos da tecnologia da informação e comunicações incluindo a avaliação de desempenho e gestão de riscos.

De uma forma mais acadêmica PERES (2010) define:

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

Devido ao alto grau de informatização e automação das organizações, bem como o alto grau de dependência destas com as comunicações, os riscos relacionados a TI aumentaram de tal forma que para muitas empresas a TI representa a área de maior risco operacional. A seguir um demonstrativo de perdas operacionais ocasionadas por falhas na área de TI em vários segmentos nos Estados Unidos, conforme as seguintes fontes: (1) D&T Revenue Assurance Survey, PWC, KPMG Publicações, (2) BIS – Quantitative Impact Study, (3) GAO Report 1999, IIC Report 2001 e (4) 2001 National Secure Survey – Universidade da Flórida.

Tabela 1- Impactos gerados por falhas nos sistemas de informação

Tipo de Negócio	Impacto gerado por falhas nos sistemas de informação
Telecom	Em torno de 5 a 10% da receita é perdida Isto representa U\$ 15 a 30 bilhões por ano (1)
Bancos	30 Bancos reportaram uma perda operacional em torno de 2,6 bilhões de euros; (2)
Seguros	O programa Medicare dos Estados Unidos

	perdeu entre 7% a 10% do seu orçamento devido a erros de integridade nas informações. (3)
Varejo	Empresas de varejo nos Estados Unidos perderam em torno de U\$ 5,6 bilhões em 2001 devido a erros administrativos (4)

Fonte: www.tiexames.com.br

Em 2002 uma pesquisa realizada pelo Gartner descobriu que 20% de todos os gastos realizados com TI foram desperdiçados, uma descoberta que representa, em base global, uma perda em torno de U\$ 600 bilhões (Gartner – The elusive bussiness value of IT – 2002). Em 2004 uma pesquisa realizada pela IBM com CIOs das maiores empresas listadas pela revista Fortune revelou que na média, os CIOs acreditavam que 40% dos investimentos em TI não gerariam nenhum retorno para suas empresas. Em 2006 um estudo realizado pelo Standish Group descobriu que apenas 35% dos projetos de TI são concluídos com sucesso.

Uma análise mais profunda da área de TI, nos mostra que os principais problemas constatados em relação aos investimentos são os relativos ao insucesso dos projetos e os gerados pela definição inadequada do tratamento dos riscos associados aos ativos de informação, ambos gerando as maiores perdas.

É de fundamental importância sejam resolvidas as seguintes questões: alinhar a TI ao negócio, entregar valor (soluções que atendam as necessidades), gerenciar a segurança da informação, demonstrar retorno aos investimentos, gerenciar a complexidade da infraestrutura de TI, executar os projetos dentro do prazo, custo e qualidade, gerenciar os ANS (acordos de nível de serviço), manter a alta disponibilidade dos serviços de TI, garantir a continuidade do negócio e estar em conformidade com as normas e regulamentos pertinentes.

Algumas destas questões precisam ser respondidas adequadamente durante o acompanhamento das atividades de TI : os objetivos já foram definidos ? a TI está entregando o que se espera ? quais recursos precisam ser gerenciados e priorizados ? como dirigir os processos de TI e como definir controles para os

mesmos ? como definir papéis e responsabilidades ? como estabelecer metas utilizáveis pelo negócio e pela TI ?

Todas estas perguntas podem ser resolvidas mediante a implantação de uma estrutura de Governança de TI. As organizações podem ter 3 níveis de governança: Governança Empresarial, Governança Corporativa e Governança de TI.

A Governança Empresarial, segundo o CIMA – Chartered Institute of Management Accountants:

“é um conjunto de responsabilidades e práticas exercitadas pela alta administração e gerências executivas com o objetivo de fornecer o sentido estratégico , assegurando-se de que os objetivos estejam sendo alcançados, verificando se os riscos estão sendo controlados apropriadamente e se os recursos da empresa estão sendo utilizados com responsabilidade”.

Segundo o IBGC – Instituto Brasileiro de Governança Corporativa:

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

Já a Governança de TI, segundo o IT Governance Institute:

“É de responsabilidade da alta administração (incluindo diretores e executivos) na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização” A Governança de TI sustenta a Governança Empresarial e Corporativa.

Uma Governança de TI efetiva deve apresentar soluções no que se refere a: Quais decisões precisam ser tomadas para garantir a governança da TI ? Quem deve tomar estas decisões ? Como monitorá-las ? Os serviços de TI são entregues de acordo com as prioridades do negócio ? Os custos são otimizados ? A segurança da informação está recebendo o tratamento adequado ? As medições de desempenho detectam problemas a tempo de resolver ? É possível associar o desempenho da TI as metas do negócio ?

As decisões podem ser distribuídas em cinco domínios: princípios de TI (Como a TI será usada no negócio), estratégias para Infraestrutura de TI, arquitetura de TI , necessidades de aplicações de negócio (aplicações que necessitam ser adquiridas ou desenvolvidas internamente) e Investimentos em TI . (WELL AND ROSS , 2004).

As áreas de foco da Governança de TI são: alinhamento estratégico, entrega de valor, gerenciamento de riscos, gerenciamento de recursos e monitoramento do desempenho. A Governança de TI se preocupa com as operações, o desempenho dos negócios transformando e adequando a TI para o atendimento dos requisitos do negócio. A Governança de TI tem como patrocinadores a direção e os executivos de TI.

A governança de TI nada mais é do que uma estrutura bem definida de relações e processos que controla e dirige uma organização no atual cenário de forças econômicas em extrema competição. O foco é permitir que as perspectivas de negócios, de infra-estrutura de pessoas e de operações sejam levadas em consideração no momento de definição do que mais interessa à empresa, alinhando a tecnologia da informação à sua estratégia.

A estratégia de implantação dos princípios de governança de TI busca superar a carência de mecanismos que possam gerenciar e controlar a utilização de TI de maneira a criar valor e trazer retornos consistentes à organização e criar formas de controlar e quantificar os resultados das otimizações. Estudo realizado pelo MIT (Massachusetts Institute of Technology) com 250 empresas em 23 países revelou que as empresas com governança de TI melhor do que a média conseguem um retorno pelo menos 20% maior sobre seus bens do que as organizações com uma governança mais fraca.

A utilização de um modelo de Governança de TI numa organização, mais especificamente o CobiT, é normalmente implementado com a expectativa de melhorar os processos de TI da organização, para obtenção do alinhamento da área de TI com o negócio, além da entrega de valor à organização, redução de custos com a área de TI, maior segurança, conformidade com normas regulatórias e manutenção e disponibilidade dos serviços de TI.

2.2. COBIT – OBJETIVOS DE CONTROLE PARA INFORMAÇÕES E TECNOLOGIAS RELACIONADAS

O acrônimo Cobit que significa Control Objectives for Information and related Technology - Objetivos de Controle para informações e Tecnologias relacionadas foi desenvolvido pela ISACA e é mantido atualmente pelo ITGI (IT Governance Institute). É um modelo focado no negócio, orientado a processos de TI (34 processos), baseado em controles e indicadores. É um framework adotado mundialmente, ele é distribuído gratuitamente, através deste modelo os objetivos do negócio são mapeados e relacionados com os processos, atividades e metas de TI, fornecendo desta maneira suporte tanto a governança quanto ao gerenciamento de TI. Como um modelo de controle ele pode ser utilizado em qualquer porte de empresa, plataforma de TI e padrão de sistemas.

O CobiT trata de todas as iniciativas e princípios de governança de TI, além de propiciar integração com os Sistemas de Gestão Específicos, como a ISO 9001 (Qualidade), ISO 27001 (Segurança da Informação), ITIL e ISO 20000 (Gestão de Serviços) e CMM/CMMI (Qualidade de Software), entre outros.

Ele diz “o que fazer” mas não “como fazer”. Primeiramente, é preciso lembrar que o Cobit não é um padrão de mercado da área de TI, mas sim, um sumário de melhores práticas, necessitando que a empresa consiga identificar, dentro do seu contexto de atuação de mercado, cultura, objetivos estratégicos, conformidades com leis e regulamentos e estrutura da área de TI, quais controles ditados pelo framework melhor atendem às necessidades e realidade da organização.

Ele funciona como um guarda-chuva fornecendo controles que mapeiam os principais frameworks de TI, incluindo as normas ISO 9001, ISO 20000 e ISO 27001 e ainda tem os cinco requisitos que um framework de controle deve ter: foco no negócio , orientado a processos, linguagem comum, atendimento a requisitos regulatórios e com aceitabilidade geral.



Figura 1 – Funcionamento do Cobit em relação aos frameworks de TI

Os componentes do Cobit podem ser resumidos na figura abaixo:

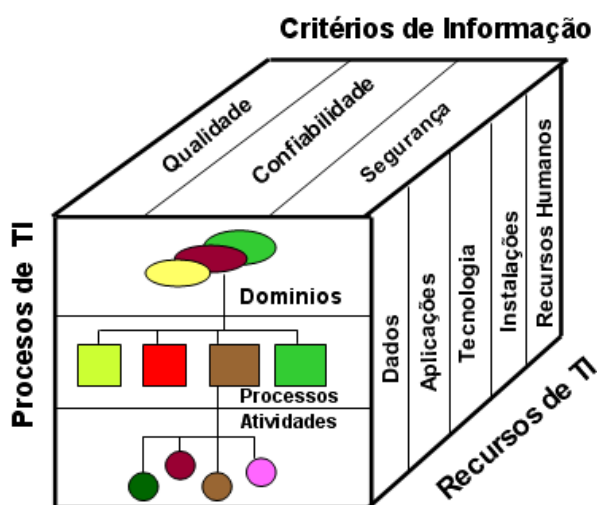


Figura 2 - Componentes do Cobit

CRITÉRIOS DE INFORMAÇÃO

Para satisfazer os objetivos de negócio, as informações precisam estar em conformidade com os critérios chamados requisitos de negócio.

- Requisitos de Qualidade
 - Qualidade
 - Custo
 - Entrega
- Requisitos Fiduciários (Relatório do COSO)
 - Eficácia e eficiência das Operações
 - Confiabilidade das Informações
 - Conformidade com Leis e Regulamentos

- Requisitos de Segurança
 - Confidencialidade
 - Integridade
 - Disponibilidade

RECURSOS DE TI

- **Aplicações:** sistemas automatizados e procedimentos manuais para processar informações
- **Informação:** os dados de todos os formulários de entrada, processados e exibidos pelos sistemas de informação, podendo ser qualquer formulário que é usado pelo negócio.
- **Infra-estrutura:** inclui hardware, sistemas operacionais, sistemas de banco de dados, rede, multimídia, etc. É tudo que é necessário para o funcionamento das aplicações.
- **Pessoas:** pessoal necessário para planejar, organizar, adquirir, implementar, entregar, dar suporte, monitorar e avaliar os sistemas de informação e serviços. Eles podem ser internos ou terceirizados.

PROCESSOS DE TI

A estrutura COBIT trata a tecnologia da informação em quatro dimensões, sendo que cada dimensão é composta por um conjunto de processos,, a seguir serão apresentadas as quatro áreas e seus respectivos processos:

- Planejamento e organização – estratégia, a tática e a identificação de como contribuir para melhorar a realização dos objetos organizacionais. Para tal precisa ser planejada, e administrada sob perspectivas diferentes. Como a organização e a infraestrutura de TI devem estar instaladas. As questões a serem respondidas neste domínio são: A área de TI e as áreas de negócio tem estratégias alinhadas ? A empresa atinge um nível ótimo de utilização dos recursos de TI ? Todos os funcionários da empresa conhecem os objetivos da TI ? Os riscos de TI são

entendidos e gerenciados ? A qualidade dos serviços de TI é apropriada para empresa ? Os processos que integram este domínio são:

- PO1 Definir um Plano Estratégico de TI
- PO2 Definir a Arquitetura de Informação
- PO3 Determinar a Direção Tecnológica
- PO4 Definir Processos de TI, Organização e Relacionamento
- PO5 Gerenciar o Investimento em TI
- PO6 Comunicar Metas e Diretivas Gerenciais
- PO7 Gerenciar Recursos Humanos
- PO8 Gerenciar Qualidade
- PO9 Avaliar e Gerenciar Riscos
- PO10 Gerenciar Projetos

Aquisição e Implementação – Para que a tecnologia da informação de fato tenha um papel crucial na estratégica organizacional é preciso que seja adquirido, desenvolvidas e implementadas as soluções em TI, e que as mesmas estejam integradas aos processos da organização. Mudanças e manutenção nos sistemas existentes são cobertas neste domínio para garantir que as soluções continuem atingindo aos objetivos do negócio. As questões a serem resolvidas pelo domínio são: Os novos projetos de TI apresentam soluções que se adéquam aos requisitos do negócio ? Os novos projetos de TI cumprem prazos e orçamento ? Os novos sistemas funcionam corretamente quando são implantados ? As mudanças realizadas na área de TI são adequadamente planejadas para que não causem impactos negativos ? Os projetos que integram o domínio são:

- DS1 Definir níveis de Serviços
- DS2 Gerenciar Serviços de Terceiros
- DS3 Gerenciar Performance e Capacidade
- DS4 Garantir Continuidade dos Serviços
- DS5 Garantir Segurança dos Sistemas
- DS6 Identificar e Alocar Custos
- DS7 Educar e Treinar usuários

- DS8 Gerenciar Service Desk e Incidentes
- DS9 Gerenciar a Configuração
- DS10 Gerenciar Problemas
- DS11 Gerenciar Dados
- DS12 Gerenciar os Ambientes Físicos
- DS13 Gerenciar Operações

Entrega e suporte – É necessário apresentar os serviços e os resultados dos vários processos, que são requeridos pelo negocio. Essas informações devem atender os requisitos de segurança. Esse domínio também inclui o processamento de dados pelos sistemas e aplicativos. Para poder entregar os serviços é necessário criar processos de suporte. As questões a serem resolvidas pelo domínio são : Os serviços de TI estão alinhados com as prioridades do negócio ? Os custos de TI estão adaptados às necessidades ? Os custos de TI estão otimizados ? As pessoas estão treinadas e aptas a utilizar os recursos de TI de forma produtiva e segura ? A segurança da informação está implantada ? Os processos integrantes deste domínio são:

- DS1 Definir níveis de Serviços
- DS2 Gerenciar Serviços de Terceiros
- DS3 Gerenciar Performance e Capacidade
- DS4 Garantir Continuidade dos Serviços
- DS5 Garantir Segurança dos Sistemas
- DS6 Identificar e Alocar Custos
- DS7 Educar e Treinar usuários
- DS8 Gerenciar Service Desk e Incidentes
- DS9 Gerenciar a Configuração
- DS10 Gerenciar Problemas
- DS11 Gerenciar Dados
- DS12 Gerenciar os Ambientes Físicos
- DS13 Gerenciar Operações

Monitoração e Avaliação – E a avaliação cotidiana de todo o processamento para assegurar a qualidade e conformidade com os controles requeridos, cuidando da

administração do processo de controle da organização de TI. Este domínio estabelece o gerenciamento de desempenho, monitoramento dos controles internos, conformidade regulatória e de governança. As questões a serem respondidas pelo domínio são: o desempenho da TI é mensurado para detectar problemas antes que eles aconteçam ? O gerenciamento garante que os controles internos sejam efetivos e eficazes ? Pode o desempenho de TI ser combinado com os objetivos do negócio ? Riscos, controles, conformidades e desempenho são medidos e reportados ? Os processos integrantes do domínio são:

- ME1 Monitorar e Avaliar a Performance de TI
- ME2 Monitorar e Avaliar Controle Interno
- ME3 Assegurar Conformidade Regulatória
- ME4 Fornecer Governança de TI

O modelo Cobit tem dois grandes focos, a saber: Fornecer informações necessárias para suportar os objetivos e requisitos de negócio e tratar informações como sendo o resultado combinado de aplicações de TI e recursos que precisam ser gerenciados por processos de TI. Os principais elementos orientadores de gestão do modelo Cobit são: os FCS (Fatores Críticos de Sucesso), KGI (Indicadores Chaves de Metas), KPI (Indicadores Chave de Performance) e Modelo de Maturidade.

Os FCS indicam o que é mais importante a fazer para garantir que os processos de TI atingirão suas metas, por exemplo: processo definido e documentado, políticas definidas e documentadas, contabilização e rastreabilidade, forte compromisso e apoio da administração, etc..

Os Indicadores Chaves de Metas KGI (acrônimo de Key Goal Indicators) indicam se um processo de TI alcançou a sua meta a nível de critérios de informação. Este tipo de indicador é usado após a execução do processo, não durante o processo.

Os Indicadores Chaves de Performance KPI (acrônimo de Key Performance Indicator) determinam quanto o processo de TI conseguiu atingir em relação aos

objetivos. São indicadores que podem avaliar o processo enquanto ele está em execução, desta forma permiti tomar ações corretivas durante o processo.

O Modelo de maturidade é uma medida que possibilita uma organização a classificar sua maturidade para um certo processo de inexistente (0) à otimizado (5). Os modelos de maturidades fazem parte das diretrizes de Gerenciamento, e podem ser utilizados para fazer comparações de maturidade com outras empresas.

Tabela 2 - Modelo de Maturidade Genérico

0 Inexistente	Não existem controles
1 Inicial	Já existem processos, só que não tem documentos, não existe padrões.
2 Repetível	Processos padronizados, só que falta documentação, comunicação
3 Definido	Os processos são formalizados, existe documentação, treinamento, comunicação definida.
4 Gerenciado	Processos em aperfeiçoamentos, já fornecem as boas práticas. Mas faltam ferramentas de automação,
5 Otimizado	Os processos já estão refinados a partir das melhores práticas identificadas. Já existe institucionalização das melhores práticas.

Nos próximos capítulos serão apresentados os Sistemas de Gestão definidos pelas normas ISO 9001, 27001 E 20000, que adotados em conjunto com o modelo Cobit tornam-se cada vez mais um padrão na TI.

2.3. BENEFÍCIOS E IMPACTOS GERADOS PELA ADOÇÃO DA GOVERNANÇA EM TI DE FORMA INTEGRADA COM OS DEMAIS SISTEMAS DE GESTÃO.

A adoção do modelo Cobit na Governança em TI pelo simples fato do provimento dos princípios orientadores oferece benefícios tanto às empresas quanto aos profissionais de TI das mesmas, como apresentado a seguir:

1. **Responsabilidade**, com o estabelecimento de estruturas organizacionais adequadas, papéis, responsabilidades e níveis de autoridade para a tomada de decisão e execução de tarefas, temos uma empresa operacionalmente funcional e equipe treinada e com conhecimento de suas responsabilidades e atividades.
2. **Estratégia**: a tradução dos requisitos do negócio em metas para TI faz com que a TI tenha um planejamento baseado nestas metas e conseqüentemente ajustado às necessidades e capacidade da organização.
3. **Aquisições**: os projetos de TI passam a ser vistos como parte do programa de mudança organizacional, a conseqüente revisão nos processos de negócio e treinamento da equipe melhora o desempenho da organização.
4. **Desempenho**: com a definição das metas de desempenho as necessidades de melhoria passam a ser bem determinadas e quantificadas. Há uma determinação no nível de atingimento das metas.
5. **Conformidade**: a implantação de políticas e procedimentos com o objetivo de assegurar o atingimento das metas, mitigação de riscos e alcance da conformidade normativa, favorece o desenvolvimento dos recursos humanos, principalmente na qualificação de suas atividades.
6. **Comportamento Humano**: como a Governança em TI promove mudanças, nesta nova situação são requeridas mudanças comportamentais e culturais tanto entre os colaboradores como entre parceiros e fornecedores.

Integradamente com os sistemas de gestão da organização, a adoção de um modelo de governança em TI, como o Cobit traz como maior benefício a demonstração do valor que a TI entrega ao negócio e para isso estabelece um relacionamento entre causa e efeito entre os tipos de métricas adotados. Os indicadores de performance medem como a organização está fazendo, são os indicadores de tendência. As medidas de resultado medem o que tem sido feito. Desta forma todos os processos dos sistemas de gestão são medidos e avaliados continuamente.

A utilização destes mecanismos requer a adequação dos controles internos às conformidades exigidas por diferentes órgãos reguladores (como a SOX, a Basiléia II e a CVM), melhorar a qualidade e simplificar o trabalho, gerenciar os processos (revisão, suporte, orientação e controle), além de redesenhar e padronizar os processos de modo a garantir a gestão inteligente dos negócios, gestão inteligente significa acréscimo no valor agregado.

A adoção de um modelo de governança como o Cobit, facilita o processo de gestão da TI e aumenta o profissionalismo da área (com a criação de indicadores de desempenho e a auto-avaliação), de forma que a TI passa a conhecer os requisitos do negócio, além de focar suas metas em decisões estratégicas da corporação.

A governança de TI integrada com o sistema de gestão da qualidade permite o aumento da eficiência da utilização da infra-estrutura de TI, através de um maior monitoramento e controle da tecnologia. Os mecanismos proporcionam também redução de incidentes, maior estabilidade e disponibilidade dos sistemas, além de eliminar os sistemas paralelos e qualificar o pessoal. Os controles de documentação e registros adotados pela ISO9001 favorecem a integração dos demais sistemas de gestão e a aplicação dos objetivos de controle e indicadores da governança. Os processos além de definidos passam a ser gerenciados, as responsabilidades ficam claras e a organização se compromete como um todo..

O modelo de governança de TI integrado ao um sistema de gestão de segurança da informação possibilita implementar políticas corporativas para melhorar a segurança da informação interna e externa. O desenvolvimento de procedimentos para garantir segurança (como plano diretor de segurança, de recuperação de desastres, de contingências e de continuidade de negócios) se torna possível com a estruturação da área de segurança da informação. A gestão dos ativos e riscos inerentes com avaliações programadas e análise através dos objetivos de controle da governança asseguram a efetividade da proteção dos ativos e mitigação dos riscos.

A integração entre governança (Cobit) e o sistema de gestão de serviços de TI possibilita uma melhora na performance, no controle, no monitoramento e na

qualidade destes, independente de serem prestados internamente, externamente ou por terceiros.

A principal observação a ser feita ao se implantar um modelo como este, para a governança de TI, é que ele vai determinar o que fazer, e não o como fazer. No entanto é indispensável a adoção do modelo de gestão por processos com indicadores e metas de controle que definirão o nível de desempenho;

CAPITULO 3 – O SISTEMA DE GESTÃO DA QUALIDADE APLICADO A TI – A NORMA ISO-9001

3.1. O QUE É A ISO?

A ISO – “ International Organization for Standardization é uma organização sediada em Genebra, Suíça, fundada em 1946. O propósito da ISO é desenvolver e promover normas que possam ser utilizadas em todo o mundo.

Cerca de 157 países integram esta importante organização especializada em padronização. Os membros são entidades normativas nacionais. No Brasil ela é representada pela ABNT – Associação Brasileira de Normas Técnicas.

A sigla ISO se originou da palavra isonomia.

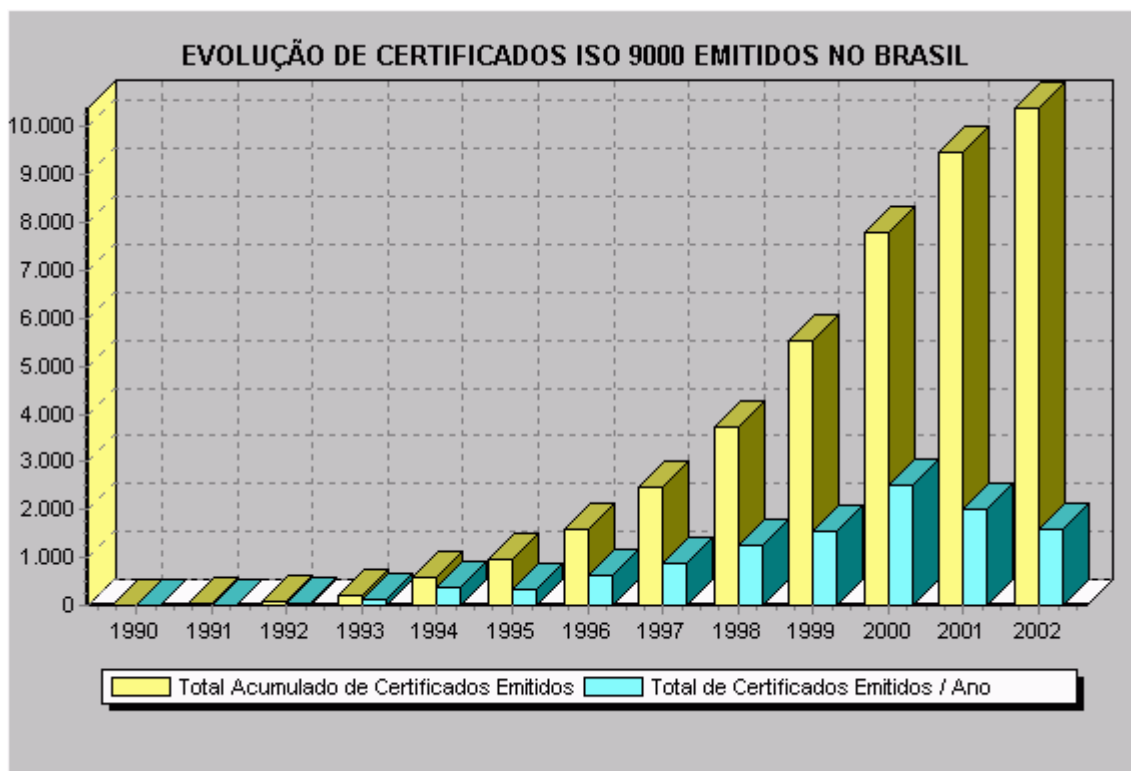
As normas ISO que tratam da implementação de Sistemas de Gestão são:

- ISO/IEC 27001 – Segurança da Informação
- ISO/IEC 20000 – Gestão em TI
- ISO 9001 – Qualidade
- ISO 14001 – Ambiental
- OHSAS 18001 – Segurança e Saúde Ocupacional
- TL 9000 – Telecomunicações
- TS 16949 – Automotiva
- SAE AS 9100 – Aeroespacial
- ISO 22001 – Alimentos

A série ISO 9000, se refere ao sistema de gestão da qualidade, esta série é constituída por três normas destinadas ao “Gerenciamento da Qualidade” e a “Qualidade Assegurada”. Estas normas são genéricas, elas definem quais elementos devem ser implementados, e não a como devem ser implementados.

Desde a década de 90, o Sistema de Gestão da Qualidade baseado na norma ISO 9000, vem se tornando padrão no mundo. A Tabela 3 apresenta a evolução das certificações no Brasil.

Tabela 3- Evolução de Certificados ISO 9000 no Brasil



Fonte: ABNT

3.2. O SISTEMA DE GESTÃO DA QUALIDADE ISO 9000

A série de normas ISO 9000 é um conjunto de normas e diretrizes internacionais para sistemas de gestão da qualidade. Desde sua primeira publicação em 1987 tem aceitação mundial como a base para sistemas de qualidade. Tanto a norma ISO 9000 como a ISO 14000 são consideradas as normas genéricas para sistemas de gestão.

O que é qualidade? ISHIKAWA(1998, p. 44), considerado o maior teórico da qualidade no Japão, assim a definia:

“A qualidade significa qualidade de trabalho, qualidade de serviços, qualidade de informação, qualidade de processo, qualidade de divisão, qualidade de pessoal, incluindo operários, engenheiros, gerentes e executivos, qualidade de sistema, qualidade de empresa, qualidade de objetivos etc. (...) e a qualidade em todas as suas manifestações.”

Em concordância a estes conceitos vem o pensamento de Joseph Juran sobre o desenvolvimento do conceito de gestão da qualidade total:

“A expressão produto inclui bens, serviços e informações trocadas entre a empresa e o mercado (fornecedores e clientes), tanto quanto entre os departamentos de pessoas dentro da organização. A expressão processo inclui processos de fabricação, bem como processos administrativos ou de vendas. E a expressão cliente envolve, além do público externo, que compra os produtos da empresa, todas as pessoas e grupos impactados pelas ações da empresa, estejam fora ou dentro dela. Somos todos fornecedores e clientes. Cada pessoa e setor, dentro da organização, tem por objetivo gerar produtos capazes de satisfazer as necessidades de outras pessoas ou setores, com máximo desempenho e mínimo custo. (...) Se qualquer fornecedor gera um produto para o qual não existe um cliente específico, isso é um desperdício que irá onerar o produto final da empresa (JURAN, apud MIRANDA, 1994, p. 6).”

Estes conceitos por si só já justificariam a adoção de um sistema de gestão da qualidade para qualquer tipo e porte de organização. Os sistemas de gestão da qualidade baseados na ISO 9001:2008 são sistemas baseados em processos, cujo foco é a melhoria contínua e a satisfação dos clientes.

O sistema ISO 9001:2008 é um modelo genérico e aplicável a todos os processos da área de TI com impacto sobre os processos de gestão e governança.

Os 8 princípios de Gestão do Sistema de Qualidade são: foco no cliente, liderança sobre objetivos comuns, envolvimento de todos, considerar o impacto de decisões em outros processos, melhorar melhorar ..., decidir após ter os dados e benefícios mútuos entre clientes e fornecedores.

A norma ISO 9001:2008 especifica requisitos para um Sistema de Gestão da Qualidade de uma organização, permitindo que ela demonstre a sua capacidade de fornecer ao cliente o produto que satisfaça os requisitos regulamentares e legais aplicáveis, e visa melhorar a satisfação dos clientes através da aplicação eficaz do sistema, incluindo processos para melhoria contínua e a garantia de conformidade

com as especificações do cliente e os requisitos regulamentares e legais aplicáveis. Todos os requisitos da norma ISO 9001:2008 são genéricos e destinam-se a ser aplicados a todas as organizações, independentemente do tipo, tamanho e produto fornecido.

Como forma de atender o propósito de revisão constante das normas publicadas pela ISO, e considerando todo o conhecimento e experiência da comunidade que utiliza Sistemas de Gestão, a norma ISO 9001:2008 deve estar com os seus requisitos adequados às novas necessidades das empresas. O trabalho de revisão e adequação do texto da norma ISO 9001, continua orientado para as organizações que pretendem se beneficiar com a implementação e operacionalidade de um Sistema de Gestão da Qualidade, porém dentro de uma maior aproximação com a norma ISO 14001 (Sistema de Gestão Ambiental), isto não poderia ser diferente uma vez que a preocupação com o meio ambiente está cada vez mais presente em todas as áreas. A versão 2008 da norma apresenta pequenas, mas consideráveis mudanças no seu conteúdo, facilitando o seu entendimento, aplicabilidade e capacidade de gerar resultados sustentáveis dentro do princípio da melhoria contínua.

Como o Sistema de Gestão da Qualidade é um sistema de gestão genérico, a sua adoção proporciona importantes oportunidades de integração com os demais sistemas. As principais a serem destacadas são:

1. A estrutura e diretrizes do Manual de Qualidade deve servir de base para os demais sistemas de gestão;
2. O padrão da política de qualidade deve servir como padrão para as políticas dos demais sistemas;
3. Em relação à responsabilidade da direção o planejamento das reuniões de análise crítica dos demais sistemas devem seguir os padrões das reuniões do sistema de qualidade;
4. Os requisitos de documentação devem ser os mesmos inclusive quanto a adoção de versões e modelos de documentos, lista mestra, controle de registros etc.

5. Em relação a recursos humanos, competências e treinamento manter os mesmos padrões, inclusive quanto ao mapeamento de necessidades de treinamento baseadas nos gaps identificados nas competências;
6. O planejamento de realização do produto deixa um modelo a ser seguido com os ajustes para os requisitos específicos de cada norma de sistema de gestão;
7. Manter os padrões de melhorias, ações corretivas e preventivas nos demais sistemas, considerar o conceito de Grupo de Melhoria;
8. Em relação aos processos relacionados aos clientes e satisfação dos clientes mantê-los para os demais sistemas, considerando inclusive a adoção de um banco de dados de reclamações e um responsável pela satisfação do cliente;
9. Utilizar o mesmo padrão de auditorias internas adotado pela ISO 9001 para os demais sistemas;

A implementação de um sistema de gestão baseado em um modelo oriundo das melhores práticas além de benefícios institucionais gera impactos significativos e positivos em relação aos recursos humanos envolvidos e a imagem da organização.

3.3. BENEFÍCIOS OBTIDOS E IMPACTOS GERADOS ATRAVÉS DA IMPLANTAÇÃO E CERTIFICAÇÃO DA TECNOLOGIA DA INFORMAÇÃO NA NORMA ISO 9001:2008

O principal capital de uma empresa é o humano. É de fundamental importância de se ter uma boa equipe pois a qualificação da equipe compensa eventuais desvantagens financeiras em relação às concorrentes.

Ao implementar a ISO 9001, a empresa, além de estar qualificando sua equipe, mostra ao colaborador que pensa no futuro, que não quer ficar estagnada no mercado, e acredita que melhorias devem ser realizadas e sugeridas continuamente. Assim, é muito provável que o profissional se sinta motivado a

trabalhar melhor, rever conceitos, e abraçar as mudanças que a certificação acarreta.

Uma equipe motivada faz com que fornecedores, e principalmente clientes, sejam bem tratados, novas sugestões sejam feitas e colocadas em prática com maior interesse. Ter profissionais focados e comprometidos é um diferencial considerável e a implementação de um objetivo em comum, como certificação ISO 9001 é uma forma de alinhar objetivos e pensamentos, em prol da empresa como um todo. Este, poderíamos dizer é o principal benefício indireto com a adoção de um sistema de gestão da qualidade.

Os benefícios diretos vêm da padronização em termos de documentação, definição de processos, procedimentos, controles de documentos e de registros. Melhor planejamento e controle das rotinas de trabalho, eliminando passos desnecessários. Padronização das tarefas e definição de responsabilidades obtendo-se maior segurança e agilidade aos trabalhos. Criação de um Sistema de Controle para identificação e tratamento das anomalias verificadas durante o processo, evitando retrabalhos. A realização do ciclo PDCA buscando a melhoria da qualidade, otimização dos processos e aumento da satisfação dos clientes.

A conformidade com a norma demonstra aos clientes, colaboradores e fornecedores que a organização já obteve os seguintes benefícios:

- a) Melhoria na transferência interna de conhecimentos e desenvolvimento de competências.
- b) Melhoria da moral e da motivação da equipe, já que entende o porquê faz suas atividades e se motiva.
- c) Redução dos custos com qualidade (refugos, retrabalho, devolução).
- d) Aumento da competitividade, com custo mais baixo.
- e) Aumento na satisfação dos clientes.
- f) Aumento na rentabilidade.

E esta demonstração na prática resulta em vantagem competitiva em relação aos concorrentes que não adotam a norma como paradigma de seu sistema de gestão da qualidade. Quanto aos impactos o principal é a implementação do ciclo de melhoria contínua que favorece sobremaneira o desenvolvimento das competências.

3.4. CONSIDERAÇÕES PARCIAIS

Nos primeiros capítulos, principalmente na abordagem da Governança de TI, procurou-se demonstrar a importância dos processos, indicadores e métricas em relação à melhoria contínua. A melhoria contínua, mesmo que sedimentada na gestão através de processos gerenciados têm a sua consolidação dependente do capital humano da organização.

A adoção de um sistema de gestão da qualidade tem a sua efetividade relacionada principalmente, à qualificação do pessoal envolvido nos diversos processos da organização. O processo de gestão das competências e habilidades é de fundamental importância em se tratando de sistemas de gestão da qualidade.

A característica de generalidade do sistema de gestão da qualidade é outro fator importante na integração com os demais, pois vai permitir que todos os processos relativos a documentação, manuais, ações corretivas e preventivas, etc. sejam congruentes.

CAPITULO 4 – O SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E SUA IMPORTÂNCIA – AS NORMAS ISO-27001 E ISO-27002

4.1. HISTÓRICO DAS NORMAS DA FAMÍLIA ISO 27000

Com a evolução da Tecnologia da Informação os ativos de informação passaram a ser considerados ativos de extrema importância para as organizações e como tal a necessidade de serem protegidos devido ao seu valor. Os prejuízos com problemas de segurança da informação levaram as empresas e governos a aumentar os investimentos nesta área. O roubo de computadores é um dos crimes que mais cresce internacionalmente. Cada libra de equipamento perdido ou roubado, custa 10 libras em interrupção dos negócios, o roubo de computadores custou à Industria Britânica mais de 1 bilhão de libras em 1996, segundo informações do Governo Britânico (BS 7799 Lead Auditor Course).

A partir de 1995 as normas relativas a segurança da informação foram publicadas na seguinte seqüência:

1995: BS 7799-1:1995 – Tecnologia da Informação – Código de prática para gestão da segurança da informação;

1998: BS 7799-2:1998 – Sistema de gestão da Segurança da Informação – Especificações e guia para uso;

1999: BS 7799-1:1999 – Tecnologia da Informação – Código de prática para gestão da segurança da informação;

2000: ISO/IEC 17799:2000 – Tecnologia da Informação – Código de prática para gestão da segurança da informação também referenciada como BS ISO/IEC 17799:2000;

2001: NBR ISO/IEC 17799:2001 – Tecnologia da Informação – Código de prática para gestão da segurança da informação;

2002: BS7799-2:2002 – Sistema de gestão da Segurança da Informação – Especificações e guia para uso;

Agosto/2005: NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Código de

prática para gestão da segurança da informação;

Outubro/2005: ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de segurança – Sistema de gestão da Segurança da Informação – Requisitos;

2007: Publicada a norma **ISO 27002** que substitui a norma 17799:2005

A norma ISO 27001 (Tecnologia da Informação – Sistemas de gestão de segurança da informação), trata sobre a implantação do Sistema de Gestão da Segurança da Informação (SGSI) através de requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) documentado dentro do contexto dos riscos de negócio globais da organização. Atualmente, essas normas são as principais referências para todos os tipos de organizações (empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos) que procuram tratar a questão da segurança da informação baseado em um modelo reconhecido internacionalmente. Da mesma forma como o acontecido com as normas ISO da série 9000, as empresas começaram a certificarem-se na norma BS 7799 inicialmente e após ISO 27001, hoje existindo 7058 empresas certificadas no mundo, conforme a tabela abaixo:

Tabela 4 – Numero de empresas com certificação ISO 27001

International Register of ISMS Certificates

Register Search (Version 203 December 2010) click on a letter to see the certificates

Click on [ISMS Certificates](#) to go to certificate database search facility to search for certificates by Organisation, Name or by Country.

ISMS Scopes

If you want to look at the ISMS scope of registration for the certificates listed below you can see the scopes using the Register Search (either for specific certificates or an overview of all).

Number of Certificates Per Country

Japan	3720	Bulgaria	19	Chia	3
India	509	Slovenia	17	Sibairtar	3
China	494	Philippines	15	Mecsu	3
UK	455	Pakistan	14	Argentina	2
Taiwan	401	Vietnam	14	Belgium	2
Germany	145	Iceland	13	Bosnia Herzegovina	2
Korea	106	Netherlands	13	Cyprus	2
Czech Republic	96	Saudi Arabia	13	Isle of Man	2
USA	96	Indonesia	11	Kazakhstan	2
Hungary	71	Kuwait	11	Morocco	2
Italy	64	Norway	10	Ukraine	2
Spain	63	Portugal	10	Armenia	1
Poland	58	Russian Federation	10	Bangladesh	1
Malaysia	46	Sweden	9	Belarus	1
Ireland	37	Colombia	8	Denmark	1
Thailand	37	Bahrain	7	Ecuador	1
Austria	35	Iran	7	Jersey	1
Hong Kong	33	Switzerland	7	Kyrgyzstan	1
Greece	30	Canada	6	Lebanon	1
Romania	30	Croatia	6	Luxembourg	1
Australia	29	South Africa	5	Macedonia	1
Singapore	29	Sri Lanka	5	Mauritius	1
Mexico	24	Dominican Republic	4	Moldova	1
Brazil	23	Egypt	4	New Zealand	1
Slovakia	23	Lithuania	4	Sudan	1
Turkey	20	Oman	4	Uruguay	1
UAE	20	Peru	4	Yemen	1
France	19	Qatar	4	Total	7058

Fonte: ISMS

Paralelamente as iniciativas de normalização técnica, os governos também tem editado legislação a respeito como as Leis 10.683 de 2009, Decreto 5.772 de 2006 e Decreto 6.931 de 2009 do Governo Federal do Brasil. Para se ter uma idéia do tamanho do problema de Segurança da Informação utilizaremos os dados oficiais do Departamento de Segurança da Informação e Comunicações da Coordenação de Inteligência Federal: Existem aproximadamente 12.000 sites com o domínio .gov, (+de 6 milhões de páginas).

Nas redes federais de dados temos 2100 tentativas de invasão por hora. No ano de 2009 em uma rede tivemos aproximadamente 4,5 milhões de incidentes e 200 malwares analisados por mês. Cerca de 92% dos malwares analisados, segundo CTIR Gov 2009, tem como objetivo roubo de informações (60 % informações bancárias, 25% informações pessoais e 7% informações do INFOSEG). No primeiro semestre de 2011 a imprensa noticiou incidentes relativos a segurança da informação em muitos portais corporativos e governamentais.

Em relação a acordos internacionais o Brasil já assinou acordos de cooperação relativos a segurança da informação com: Rússia, Portugal, Espanha e França e está em fase de negociação com: Israel, Estados Unidos, Luxemburgo, Itália, Rep. Tcheca, Ucrânia e Noruega.

São dois os princípios básicos que devem ser observados para se garantir a Segurança da Informação e Comunicações bem como das infraestruturas críticas no ciberespaço:

1. Reduzir vulnerabilidades impedindo ou dificultando ataques;
2. Em caso de ataque, garantir uma rápida recuperação e funcionamento dos sistemas de informação e infraestruturas críticas afetadas.

Toda a iniciativa em segurança da informação, desde a elaboração de políticas até a construção de um sistema de gestão da segurança das informação tem como ponto de partida o inventário dos ativos de informação e o processo de gestão dos riscos, conforme será visto no detalhamento do Sistema de Gestão da Segurança da Informação – SGSI.

4.2. O SISTEMA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO

Como os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma geridas para proporcionar confidencialidade, integridade e disponibilidade dos ativos de informação, que conforme a norma NBR ISO/IEC 27002 podem ser assim definidos:

Confidencialidade – garantia que a informação somente é acessível por pessoas explicitamente autorizadas a terem acesso; quem acessa um ativo de informação deve ser identificado e autenticado.

Disponibilidade – garantia de que as pessoas autorizadas tenham acesso as informações e seus ativos correspondentes sempre que necessário;

Integridade – salvaguarda da exatidão e completeza da informação e dos meios de processamento.

A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização. É esperado que este e os sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (ISO 27001:2006).

O ponto de partida para um sistema de gestão da segurança da informação é uma análise dos riscos. Um risco de segurança é o potencial que uma dada ameaça irá explorar vulnerabilidades para causar perda ou dano a um ativo ou grupo de ativos. Dentro do processo de avaliação do risco temos os seguintes procedimentos: identificação e valorização dos ativos, identificação das vulnerabilidades, identificação das ameaças, avaliação de impactos que a perda de confidencialidade, integridade e disponibilidade nos ativos pode causar, análise e avaliação dos riscos e priorização dos riscos. A partir da avaliação dos riscos temos o processo de tratamento dos mesmos que envolve a mitigação, transferência, eliminação ou

aceitação do risco residual. Todos estes aspectos são abordados no Sistema de Gestão da Segurança da Informação.

Os fatores críticos do sucesso da implementação de um SGSI são: comprometimento e apoio visível de todos os níveis da direção; provisão de recursos para as atividades de Gerenciamento de Segurança da Informação; divulgação, conscientização, educação e treinamento adequados; política de segurança da informação, objetivos e atividades refletindo os objetivos do negócio e bom entendimento dos requisitos de segurança da informação, avaliação de risco e gerenciamento de risco.

A norma ISO 27001, como a maioria dos sistemas de gestão, prevê a abordagem por processos utilizando o modelo PDCA:

“Esta Norma adota o modelo conhecido como *"Plan-Do-Check-Act"* (PDCA), que é aplicado para estruturar todos os processos do SGSI. A figura 1 ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas. A figura 1 também ilustra os vínculos nos processos apresentados nas seções 4, 5, 6, 7 e 8”

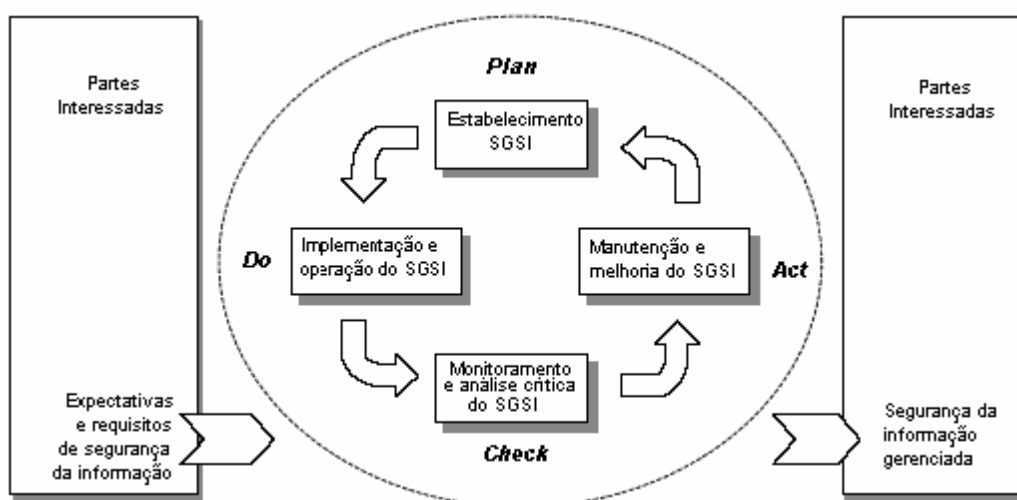


Figura 3 - Modelo PDCA aplicado aos processos do SGSI

Plan (planejar) (estabelecer o SGSI) Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da

segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Do (fazer) (implementar e operar o SGSI) Implementar e operar a política, controles, processos e procedimentos do SGSI.

Check (checar) (monitorar e analisar criticamente o SGSI)

Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

Act (agir) (manter e melhorar o SGSI) Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A norma prevê ainda:

“4.1 Requisitos gerais

A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta. Para os efeitos desta Norma, o processo usado está baseado no modelo de PDCA mostrado na figura”

Os requisitos para o estabelecimento do SGSI são especificados pelo item 4.2.1. da norma, e tem como produto final a declaração de aplicabilidade. A declaração de aplicabilidade provê um resumo das decisões relativas ao tratamento de riscos. A justificativa das exclusões estabelece uma checagem cruzada comprovando que nenhum controle foi omitido inadvertidamente.

A ISO/IEC 27001:2005 é integrada por 39 objetivos de controle e 133 requisitos, que devem ser abrangidos pelo SGSI e que são objeto de verificação nas auditorias internas e de certificação. No caso de algum dos controles não se aplicar a organização o mesmo deverá estar relacionado na declaração de aplicabilidade como não aplicável. Os requisitos estão relacionados no anexo A da norma.

A norma ISO 27002, Tecnologia da Informação – Código de prática para gestão da segurança da informação oferece uma visão abrangente dos controles que podem ser utilizados em uma organização, como:

- Política de segurança
- Segurança organizacional
- Classificação e controle de ativos de informação
- Segurança relacionada às pessoas
- Segurança ambiental e física
- Gerenciamento das operações e comunicações
- Controle de acesso
- Desenvolvimento e manutenção de sistemas
- Gestão de incidentes de segurança
- Gestão da continuidade do negócio
- Conformidade com as diretrizes da empresa

Um exemplo desses controles, é a classificação e controle de ativos de informação. É necessário realizar um inventário de todos os ativos de informação existentes na organização, pois somente assim é possível ter um panorama das ameaças que cada ativo sofre, bem como a sua sensibilidade e importância. Além disso, é necessário implantar um Plano de Contingência para assegurar a continuidade dos negócios em caso de desastres maiores.

A documentação do SGSI deve incluir:

- a) Declarações documentadas das políticas e dos objetivos do SGSI
- b) O escopo do SGSI
- c) Procedimentos e controles que apóiam o SGSI
- d) Uma descrição da metodologia de análise/avaliação de riscos
- e) O relatório de análise/avaliação de riscos
- f) O plano de tratamento de riscos
- g) Procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança da informação, e para descrever como medir a eficácia dos controles

- h) Registros requeridos pela norma
- i) A declaração de aplicabilidade

Os documentos requeridos pelo SGSI devem ser protegidos e controlados. Um procedimento documentado deve ser estabelecido para definir as ações de gestão necessárias para: aprovação, análise crítica, atualização, identificação das alterações e suas revisões, controle e disponibilidade das versões atualizadas dos documentos, disponibilidade dos documentos aos responsáveis, identificação de documentos externos, controle de transferência armazenamento e descarte de documentos, proteção da documentação e controle da utilização da mesma.

A documentação pode variar de acordo com o tamanho da organização, tipo de atividades, escopo e complexidade dos requisitos de segurança e do sistema gerenciado. Quando a norma cita apenas a palavra “procedimento” significa que o procedimento não precisa ser documentado. Se a norma disser “procedimento documentado” significa que o procedimento realmente precisa ser documentado.

O atendimento aos requisitos de documentação fica simplificado quando a organização já possui sistema de gestão da qualidade implantado, pois os requisitos de documentação e registros do sistema de qualidade são compatíveis com os demais sistemas de gestão, como vimos no capítulo anterior. Todos os registros devem ser estabelecidos e mantidos como forma de evidência da conformidade relativa aos requisitos e da operação eficaz do SGSI. Dentre os registros devemos considerar requisitos legais, contratos, acordos de nível de serviço etc.. Controles devem ser definidos, documentados e implementados para: identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição. Registros devem manter informações sobre o desempenho dos processos e de ocorrências significativas relacionadas ao SGSI. Exemplo de registro: livros de visitantes, relatórios de auditoria, formulários de autorização de acesso, etc.

No estabelecimento do SGSI segundo a norma ISO 27001, a organização deve: “Definir o escopo e os limites do SGSI nos termos das características do negócio, da organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas

para quaisquer exclusões do escopo.” Incluindo as eventuais exclusões na declaração de aplicabilidade.

A Política de Segurança da Informação deve ser elaborada de acordo com as características da organização, do negócio, sua localização ativos, tecnologias e infra-estrutura. Ela deve incluir uma estrutura para definir objetivos e estabelecer um direcionamento global e princípios para ações relacionadas com a segurança da informação. Considerar os requisitos do negócio, a legislação pertinente e as obrigações contratuais. Além de estabelecer critérios para avaliação dos riscos a política deve estar alinhada com a gestão de riscos e o SGSI. A aprovação por parte da direção e a divulgação a todas as partes interessadas é fundamental.

Na implantação do SGSI , após a realização do inventário de ativos, deve ser estabelecido um plano de tratamento de riscos que identifique ação apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança.

A implementação do plano de tratamento de riscos deverá alcançar os objetivos e controles identificados, incluindo considerações de financiamento e atribuições de papéis e responsabilidades. Deve-se implementar os controles selecionados para atender aos objetivos de controle.

Devem ser definidas as métricas para se medir a eficácia dos controles ou grupos de controles selecionados, e a metodologia de uso destas medidas pois elas devem ser usadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis. Tanto a metodologia de inventário de ativos como a de cálculo de riscos é a base para todo o sistema de gestão da segurança da informação e requisito verificado com rigor na auditoria de certificação.

A organização deve executar as atividades relativas ao Check do PDCA, ou seja a monitoração e análise crítica do mesmo. A maturidade e eficácia do SGSI são determinadas após análise das ações tomadas tanto em relação aos seus efeitos quanto aos resultados obtidos. Verificados os desvios e inconformidades três perguntas devem ser feitas: O problema foi solucionado ? Há a percepção de melhoria ? Como podemos melhorar a solução ?

No entanto é importante saber que não há melhoria contínua infinita. Cada processo pode ter ou não necessidade de melhoria e perceber isso é a fórmula para não se gastar tempo e recursos onde não é necessário. O principal dentro do processo de melhoria contínua é o envolvimento de todos os responsáveis por segurança, ou seja: alta direção, CSO, equipe de segurança da informação e demais interessados. Além das providências normais oriundas da reunião de análise crítica onde os incidentes, resultados de ações, relatórios de auditorias e demais registros são analisados os planos de segurança devem ser atualizados e principalmente os registros oriundos do processo de gestão de riscos devem ser verificados quanto a sua validade atual. As análises críticas devem ser realizadas periodicamente e devem atentar para eventuais mudanças na organização, tecnologias, infraestrutura, ameaças identificadas e eventos externos como legislação e regulamentos , requisitos contratuais e conjuntura social.

Em todo o processo de estabelecimento, implantação, operação, monitoramento, análise crítica e melhoria do SGSI a direção deve fornecer evidências de seu comprometimento: estabelecendo uma política de segurança da informação, garantindo que os objetivos e planos da segurança da informação são estabelecidos; estabelecendo papéis e responsabilidades da segurança da Informação; comunicando à organização a importância de atender aos objetivos de SI e estar em conformidade com a política da SI, com suas responsabilidades sob a lei e com a necessidade de melhoria contínua; fornecendo recursos suficientes para desenvolver, implementar, operar e manter o SGSI; decidindo critérios de aceitação de riscos e dos níveis de riscos aceitáveis e garantindo que auditorias internas sejam realizadas e conduzindo análises críticas do SGSI.

A análise crítica terá como saídas definição de ações para melhoria da eficácia do SGSI, atualização das análises e planos de tratamento de riscos, modificações necessárias nos procedimentos que afetam a segurança da informação, planejamento financeiro para as implementações necessárias e melhorias nas medições de controle.

O ANEXO A da norma, contém os objetivos de controle e todos os controles detalhados. A ISO/IEC 27001:2006 contém 39 objetivos de controle e 133 controles. Alguns controles podem não ser aplicáveis a todo sistema ou ambiente, praticáveis para todas as organizações. Os controles que não são relevantes para a organização devem ser abordados na declaração de aplicabilidade, como vimos anteriormente, as principais cláusulas de controle são:.

A.5 Política de segurança

A.6 Organização da segurança da informação

A.7 Gestão de ativos

A.8 Segurança em recursos humanos

A.9 Segurança física e do ambiente

A.10 Gerenciamento das operações e comunicações

A.11 Controle de Acesso

A.12 Aquisição, desenvolvimento e manutenção de sistemas

A.13 Gestão de incidentes de segurança da informação

A.14 Gestão da continu

idade do negócio

A.15 Conformidade

Em relação aos controles apresentados a norma ISO 27001:2005 diz:

“Nem todos os controles descritos serão relevantes para todas as situações, nem podem levar em conta o ambiente local ou condições tecnológicas e nem poderão estar presentes de uma forma adequada a todos os usuários potenciais em uma organização.”

Como vimos a segurança da informação para proteger os ativos de informação de uma grande gama de ameaças para garantir a continuidade do negócio, minimização de danos ao negócio e maximização do lucro depende de um SGSI que seja bem comunicado, documentado, consistente com as políticas da organização, seguido pelos colaboradores e apoiado pela alta direção.

4.3. BENEFÍCIOS E IMPACTOS GERADOS PELA ADOÇÃO E CERTIFICAÇÃO DO SISTEMA DE GESTÃO DA SEGURANÇA DE INFORMAÇÃO PELA TECNOLOGIA DA INFORMAÇÃO

Uma organização ao ser certificada em termos de Gestão da Segurança da Informação obtém os seguintes benefícios:

- a) **Credibilidade comercial:** O fato da organização ser reconhecida como em conformidade com a norma de segurança da informação é uma garantia para os seus clientes e parceiros da forma de que os seus dados são tratados adequadamente pela organização.
- b) **Redução de custos:** O custo de um único incidente de segurança poderá ser consideravelmente superior ao investimento em sistemas de proteção. Por outro lado a certificação pode diminuir o custo de eventuais valores de seguros que tenham como objeto a segurança dos ativos de informação da organização ou até mesmo em relação a sua capacidade de continuidade operacional.
- c) **Conformidade com normas, leis e regulamentos:** A certificação demonstra às autoridades competentes e acionistas que a organização cumpre as leis e regulamentos aplicáveis, tanto do ordenamento jurídico brasileiro como regulamentos setoriais (como o Sarbanes-Oxley, Bacen ou Basileia).
- d) **Redução do risco de incidentes de segurança:** A certificação proporciona um melhor conhecimento dos sistemas de informação, das suas vulnerabilidades e da forma como os proteger, o que resulta num aumento do nível de protecção contra riscos de negócio.
- e) **Desenvolvimento e motivação dos Recursos Humanos através de responsabilização, sensibilização e formação contínua em segurança;**
- f) **Garantia de um elevado nível de disponibilidade, confidencialidade e integridade com a redução dos riscos associados aos ativos de informação;**

4.3. CONSIDERAÇÕES PARCIAIS

Na Era da Informação, nada mais lógico do que a preocupação com a segurança da mesma. Os processos que visam assegurar a confidencialidade, integridade e disponibilidade da informação, devem ser estruturados a partir dos resultados obtidos pela análise das ameaças e vulnerabilidades identificadas nos ativos de informação pelos processos de gestão de riscos.

A gestão dos riscos em segurança da informação tem um caráter fundamental na implementação de um sistema de gestão. A sua importância é tal que gestão de riscos em segurança da informação virou uma norma específica a ISO 27005.

CAPITULO 5 – A GESTÃO DE SERVIÇOS DE TI A NORMA ISO-20000 E AS MELHORES PRÁTICAS COM A ITIL

5.1. HISTÓRICO DAS NORMAS DA FAMÍLIA ISO 20000

O governo da Inglaterra lançou a Biblioteca de Infra-estrutura de TI (ITIL) em 1989 a ITIL consiste num conjunto coerente e integrado de sete livros, cada um deles definindo as linhas diretrizes para as melhores práticas na área específica de gestão de serviços de TI. As diretrizes da mesma destinam-se a ser adaptadas por cada organização, de forma a satisfazerem as diferentes necessidades de cada uma. A ITIL é propriedade do OGC – UK Office of Government and Commerce (Gabinete de Comércio do Governo Britânico) e mantida pelo mesmo. A partir de 1990, a ITIL se torna um padrão de *fato*

O itSMF(IT Service Management Forum), fórum independente congregando profissionais de todo o mundo, foi criado em 1991 para desenvolver melhores práticas adicionais, tornando-se um *player* de destaque no desenvolvimento e promoção das melhores práticas, padrões e certificações.

Em junho de 2000 foi lançada no Reino Unido a BS 15000, a primeira norma I focada especificamente em Gestão de Serviços de TI .Esta norma, estreitamente associada à ITIL, define um conjunto de requisitos mínimos relativamente aos quais uma empresa poderá ser avaliada para determinar a eficácia dos processos de gestão de serviços de TI, proporcionando um nível de qualidade para as atividades que podem submetidas a auditoria. Os principais objetivos desta norma são: promover a adoção de uma abordagem de processos integrada para a realização de serviços gerenciados que atendam às necessidades do negócio e aos requisitos dos clientes, possibilitar o entendimento das melhores práticas, e a solução de possíveis problemas relacionados com a gestão de serviços e ajudar as organizações a gerar receita e serem eficazes através de uma gestão de serviços profissional.

A BS 15000 foi substituída pelo padrão internacional ISO/IEC 20000 após a formalização em Dezembro de 2005, tornando-se então a ISO/IEC 20000 o primeiro padrão mundial especificamente focado para o Gerenciamento de Serviços de TI. A BS 20000 compreende cinco grupos de processo chave: processos de entrega de serviços, processos de relacionamento, processos de resolução, processos de liberação e processos de controle, a maioria dos quais estão definidos na própria ITIL.

5.2. O SISTEMA DE GESTÃO DE SERVIÇOS BASEADO NA NORMA ISO 20000

A Norma ISO/IEC 20000 define os requisitos para o provedor de serviços entregar serviços gerenciados com qualidade aceitável para seus clientes. O padrão procura se fixar no ciclo de qualidade PDCA.

A norma fornece uma base para certificação a partir da implementação dos processos de gerenciamento de serviços e do seu uso de forma consistente dentro da organização, ela pode ser usada: por organizações cujo negócio é oferecer serviços, para organizações onde a qualidade do serviço de TI é essencial, por organizações que requeiram uma abordagem consistente por todos os provedores de serviços numa cadeia de fornecimento, por provedores de serviços para dar um parâmetro a seu gerenciamento de serviços de TI, como base para uma avaliação independente, por uma organização que necessite demonstrar habilidade no fornecimento de serviços que atendam aos requisitos dos clientes e por uma organização que necessite demonstrar os serviços através da aplicação efetiva dos processos para monitorar e melhorar a qualidade do serviço (ABNT ISO/IEC 2000-1:2008). É ainda mais relevante para organizações que fornecem serviços e terceirizam os serviços de TI. Para as organizações que não estão procurando a certificação, a ISO/IEC 20000 pode servir como um guia de como adotar as melhores práticas.

Seus principais objetivos são: oferecer um padrão a ser adotado baseado em processos integrados que satisfaçam os requisitos do negócio e do cliente, introduzir uma cultura de serviços baseada em metodologias que atendam requisitos do

negócio e prioridades de uma forma gerenciável, ser um modelo totalmente baseado em processos que apoiem a qualidade da entrega e suporte dos serviços, gerar valor para as organizações, melhorar a confiabilidade e disponibilidade dos sistemas e prover base de dados para os acordos de nível de serviço.

A ISO/IEC 20000 não formaliza a inclusão das práticas da ITIL, embora esteja descrito na norma um conjunto de processos de gerenciamento que estão alinhados com os processos definidos dentro dos livros da ITIL.

A sua implementação integrada com as normas ISO 9001 e ISO 27001 pode ser representada pelo gráfico apresentado na Figura 4, onde tentamos demonstrar a complementaridade dos processos das normas ISO 20000 e ISO 27001 e sua integração com processos e requisitos de documentação da norma ISO 9001 formando três sistemas de gestão integrados e certificáveis pelas 3 normas:

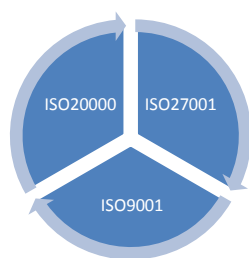


Figura 4 - Normas ISO de Sistemas de Gestão na área de TI

A ISO 20000 adota abordagem de processos. Um processo de negócio é “um conjunto de tarefas logicamente relacionadas, realizadas para conseguir um resultado definido do negócio” (PRESSMAN, 2008). A abordagem de processo identifica sistematicamente e gerencia a inter-ligação, combinação e interação de um sistema de processos dentro de uma organização. A abordagem de processo enfatiza a importância de: atendimento dos requisitos do cliente, observação dos processos quanto a geração de valor, medições de desempenho do processo e melhoria contínua.

Esta norma está dividida em duas partes, a ISO/IEC 20000-1 Parte 1: Especificação e ISO/IEC 20000-2 Parte 2: Código de Prática. A ISO/IEC 20000-1 é uma especificação formal e define os requisitos para uma organização entregar serviços gerenciados com uma qualidade aceitável para seus clientes. ISO/IEC 20000-

2:2005 é o Código de Prática e descreve as melhores práticas para os processos de Gerenciamento de Serviço dentro do escopo da ISO/IEC 20000-1.

Os processos que compõe as 5 áreas do Sistema de Gestão de Serviços de TI, segundo a norma, são:

- a) Processos de Entrega de Serviços: Gerenciamento da Capacidade, Gerenciamento de Nivel de Serviço, Gerenciamento de Segurança da Informação, Gerenciamento da Continuidade e Disponibilidade dos Serviços, Relato de Serviço e Orçamento e Contabilização para Serviços de TI;
- b) Processos de Liberação: Gerenciamento de Liberação;
- c) Processos de Resolução: Gerenciamento de Incidentes e Gerenciamento de Problemas;
- d) Processos de Relacionamento: Gerenciamento do Relacionamento do Negócio e Gerenciamento de Fornecedores
- e) Processos de Controle: Gerenciamento de Configuração e Gerenciamento de Mudanças

A norma esta sumarizada da seguinte forma:

- ✓ Prefácio
- ✓ Introdução
 - 1) Escopo
 - 2) Termos e definições
 - 3) Requisitos para um sistema de gerenciamento
 - 4) Planejando e Implementando um gerenciamento de serviço
 - 5) Planejando e implementando serviços novos ou alterados
 - 6) Processos de Entrega de serviço
 - 7) Processos de Relacionamento
 - 8) Processos de Resolução
 - 9) Processos de controle
 - 10) Processo de Liberação
- ✓ Bibliografia

O primeiro passo para a implantação da norma é a definição do escopo, a declaração de escopo deve cobrir: os serviços a serem englobados na auditoria de certificação, aspectos geográficos envolvidos, aspectos organizacionais e aspectos da infra-estrutura.

Os nomes dos processos não são relevantes e escopo da ISO/IEC 2000 precisa apenas definir os serviços gerenciados que fazem parte do escopo. A organização deve demonstrar que ela tem controle de gerenciamento de cada um dos processos da ISO/IEC 20000. O controle de gerenciamento de um processo pode ser entendido como: o conhecimento, uso, interpretação e controle das saídas e a demonstração de evidência da responsabilidade pela funcionalidade do Processo. Existem 217 requisitos dentro da norma ISO/IEC 20000 e a organização precisa cobrir por inteiro todos estes requisitos.

Após os termos e definições a norma ISO 20000 estabelece os requisitos para um sistema de gestão:

“Objetivo: Fornecer um sistema de gestão, incluindo políticas e uma estrutura para possibilitar implementação e gerenciamento eficaz de todos os serviços de TI. Os requisitos para um sistema de gestão são: responsabilidade da direção, requisitos de documentação e competência conscientização e treinamento.”

A direção deve estabelecer a política de Gerenciamento de Serviços, objetivos e planos; comunicar a importância de atingir os objetivos de Gerenciamento de Serviços e a necessidade de melhoria contínua; assegurar que os requisitos dos clientes sejam determinados e atendidos; designar o representante da direção para coordenar e administrar todos os serviços; determinar e prover recursos; administrar riscos; conduzir análises críticas da Gestão de Serviços, a intervalos planejados, para assegurar a contínua: Adequação, Conformidade e Eficácia.

A documentação deve incluir: políticas e planos de Gerenciamento de Serviços; Acordos de Nível de Serviço (ANS); Processos documentados, procedimentos e registros requeridos pela ISO/IEC 20000-1. Devem ser estabelecidos procedimentos para a criação, análise crítica, aprovação, manutenção, disposição e controle de

documentos e registros conforme os demais sistemas de gestão. A existência de um sistema de gestão da qualidade, automaticamente contempla todos estes requisitos.

A organização deve: definir e manter os papéis, responsabilidades e competências para executar os serviços com eficácia, analisar criticamente e gerenciar competências e necessidades de treinamento.

A Alta Direção deve assegurar que os colaboradores estejam conscientes da relevância e importância de suas atividades e de como eles contribuem para os objetivos do sistema de Gestão de Serviços.

O planejamento e implementação do Gerenciamento de Serviços é realizado de acordo com a metodologia PDCA, como nos outros sistemas de gestão baseados nas normas ISO.

Em relação ao planejamento(Plan), os planos devem estabelecer de forma clara: o escopo, objetivos e requisitos a serem alcançados, processos, estrutura de responsabilidades e funções, o relacionamento entre os processos, a abordagem para identificar, avaliar e gerenciar temas e riscos, a abordagem para interfacear projetos que criam ou modificam serviços, Recursos, instalações e orçamento necessários, Ferramentas para apoiar os processos e como a qualidade do serviço será administrada, auditada e melhorada.

Quanto a implementação(Do) dos planos, estes devem estabelecer as seguintes ações: alocação de recursos e orçamentos, designação dos papéis e responsabilidades, documentar e manter as políticas, planos, procedimentos e definições para cada processo, identificar e administrar riscos, gerenciar recursos humanos, instalações, orçamento, balcão de serviços e operações, acompanhar cronograma e coordenar os Processos de Gestão de Serviços.

Quanto a monitoração, medição e análise (Control), a organização deve: utilizar metodologia adequada para monitoramento e medição dos processos de Gestão de Serviços, assegurar que os métodos demonstrem que os processos atingem os resultados planejados. Quanto a análise crítica, conduzida pela direção seus em intervalos planejados, esta deve determinar se os requisitos de Gestão de Serviços: Estão em conformidade com o plano de Gestão de Serviços e a norma a ISO/IEC

20000-1 e se estão sendo implementados e mantidos eficazmente. Ainda dentro da etapa de monitoração, medição e análise, é fundamental a criação de um plano de auditoria que considere situação atual e importância das áreas auditadas, bem como comparação com auditorias prévias. A seleção dos auditores deve assegurar objetividade e imparcialidade e devem ser definidos critérios, escopo, métodos e periodicidade das auditorias.

5.3. BENEFÍCIOS OBTIDOS PELA ADOÇÃO E CERTIFICAÇÃO DO SISTEMA DE GESTÃO DE SERVIÇOS EM TI

Os principais benefícios obtidos com a adoção de um sistema de gestão de serviços baseado na norma ISO 20000 são:

- a) Melhoria da qualidade de serviço;
- b) Aumento da confiança dos clientes e do negócio;
- c) Melhoria da reputação, consistência e interoperabilidade;
- d) Garantia de melhoria contínua e de que os custos estão controlados e otimizados;
- e) Os gestores e os colaboradores compreendem melhor as suas funções, responsabilidades e os processos de trabalho;
- f) Vantagem competitiva face aos concorrentes
- g) Demonstração de capacidade de cumprimento de Acordos de Nivel de Serviço para fornecimento de serviços de TI;
- h) Auditorias imparciais e externas evidenciando, por uma terceira parte, de que o Sistema de Gestão de Serviços de TI (SGS) está em conformidade com a ISO 20000;
- i)** Certificação reconhecida internacionalmente
- j) Desenvolvimento e implementação da revisão e avaliação do SGS alinhando o mesmo com os objetivos de melhoria contínua;
- k) Aumento da satisfação dos Colaboradores através da implementação de métodos de trabalho planejados e organizados

- l) Ênfase na conformidade dos processos através da transposição dos “shoulds” em “shalls” de forma a alcançar os benefícios do Sistema de Gestão.

5.4. CONSIDERAÇÕES PARCIAIS

O Sistema de Gestão de Serviços complementa os demais sistemas de gestão já abordados no sentido de assegurar que todos os processos relativos a relacionamentos com fornecedores e clientes sejam executados e gerenciados de forma qualificada.

A complementaridade dos sistemas se dá principalmente pela abordagem por processos que se integram. Dentro do objetivo de melhoria contínua onde são adotadas as ações(Act) que visam melhorar a eficiência e eficácia dos serviços deve-se publicar uma política de melhoria dos serviços, corrigir eventuais não conformidades e gerenciar as melhorias, principalmente estabelecendo as seguintes ações: coletar e analisar dados de capacidade para “*baseline*” e “*benchmark*”, identificar, planejar e implementar melhorias, consultar todas as partes envolvidas estabelecendo objetivos para melhorias em qualidade, custos e utilização de recursos. Deve ser considerada a coleta de informações pertinentes que determinem oportunidades de melhorias e que estas sejam medidas, informadas e comunicadas. Finalmente é de fundamental importância a revisão periódica das políticas, processos, planos e procedimentos para que se mantenham atualizados e que seja assegurado que todas as ações aprovadas sejam entregues e atinjam os objetivos propostos.

CAPITULO 6 – ESTUDO DE CASO A IMPLANTAÇÃO DO SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ISO 27001 NA BRASLIGHT

A Fundação Braslight é uma entidade fechada de previdência complementar, sem fins lucrativos, regulamentada pela Lei Complementar nº 109/2001 e regida pelas normas editadas pelo Conselho Monetário Nacional (CMN), Banco Central e Ministério da Previdência Social, através da Superintendência Nacional de Previdência Complementar (PREVIC). A Braslight foi criada em 01/10/1974 com o objetivo de complementar a aposentadoria de seus participantes e de amparar suas famílias quando do seu falecimento. São suas patrocinadoras **Light S.A, Light S.E.S.A., Light Energia S.A, Light ESCO, LightGER, LIGHTCOM** e a própria Braslight.

Em setembro de 2004, como resultado de um trabalho visando dotar a Braslight de modernas práticas gerenciais, procedimentos documentados e controles eficientes e eficazes, a Fundação obteve sua primeira certificação ISO 9001:2000, que teve como escopo o processo de Concessão de Benefícios. Nos anos seguintes, novas certificações foram conquistadas nos seguintes processos: Extração de Dados para Avaliação Atuarial, a Concessão de Empréstimos e a Folha de Pagamento de Assistidos. Atualmente o Sistema de Gestão da Qualidade certificado abrange todos os processos internos que compõem a Gestão Previdenciária da Fundação.

Em 2006 a organização sentiu a necessidade da adoção de um sistema de gestão na área de TI, tendo optado pelo modelo ISO 27001. Dada a dependência de todos os sistemas certificados na ISO 9001, da área de TI, a implementação do sistema de gestão da segurança da informação teve como abrangência todos os processos de Tecnologia da Informação.

Definido este escopo, e com o auxílio de uma consultoria externa foram realizadas todas as atividades preconizadas pela norma, para implantação de um sistema de gestão, destacando-se:

- a) Criação de um plano de segurança da informação;
- b) Definição das responsabilidades em segurança da informação;

- c) Comprometimento da Alta Direção;
- d) Treinamento do quadro funcional em segurança da informação;
- e) Inventário de todos ativos de informação;
- f) Análise dos riscos em segurança da informação;
- g) Gestão dos riscos;
- h) Integração com o sistema de gestão da qualidade, com a adoção do referencial de documentação, registros, aprovação de documentos etc..
- i) Implantação de Política de Segurança da Informação (nível estratégico)
- j) Implantação das políticas de e-mail, utilização de Internet, controle de acesso, etc (nível tático);
- k) Implantação de todos os processos estabelecidos pela norma, bem como procedimentos operacionais e demais documentos necessários para o estabelecimento efetivo da segurança da informação(nível operacional);
- l) Criação de um plano de contingência e recuperação contra desastres tendo a validação do mesmo obtido o resultado de restabelecimento operacional dos principais processos num intervalo inferior a 24h;

Após a implantação completa do sistema de gestão da segurança da informação, foram realizadas as auditorias e revisões preconizadas na norma e foi assegurado que o ciclo PDCA estava sendo realizado adequadamente.

A fundação optou num primeiro momento por contratar uma auditoria de terceira parte e obter um atestado de conformidade com a norma, antes da certificação, objetivando um amadurecimento maior do sistema implantado. O atestado de conformidade com a norma foi obtido em dezembro de 2006.

Atualmente a Braslight está executando a revisão no sistema de gestão da segurança da informação, com uma meta estabelecida de certificação para o prazo de 12 meses.

Desde a obtenção do certificado de conformidade a fundação já comprovou que obteve agregação de valor dentro de suas atividades, inclusive com o aval das auditorias dos sistemas de gestão e as relativas à Governança Corporativa e de TI.

Além disso, a validação dos planos de contingência e efetivo controle dos ativos de informação, bem como, o controle rigoroso quanto a conformidade normativa, têm oferecido aos participantes dos planos de benefício, recebimento de prestação de serviços com qualidade e segurança quanto à garantia operacional e financeira da instituição a que aderiram.

6.1. CONSIDERAÇÕES PARCIAIS

O importante a destacar no caso estudado, foi a opção da alta administração da Fundação em implantar o sistema de gestão e atestar sua conformidade sem partir imediatamente para o processo de certificação.

O SGSI implantado recebeu atestado de conformidade com a norma em 2006, após 5 anos de comprovada eficiência, vai receber uma revisão de acordo com o ciclo PDCA, e a partir desta revisão e duas auditoria internas, entra em processo de certificação.

CONCLUSÃO

Este trabalho procurou mostrar, os principais sistemas de gestão adotados pela área de Tecnologia da Informação as vantagens competitivas que as empresas adquirem ao adotarem estes sistemas. O grau de dependência que as empresas têm em relação a TI nos dias de hoje, faz com que dois pontos básicos sejam focados: alinhamento estratégico e agregação de valor. Em função disso a governança de TI torna-se cada vez mais uma realidade e por isso abordamos o framework Cobit, que funciona como um guarda-chuva em relação aos demais sistemas de gestão como mostra a imagem abaixo.

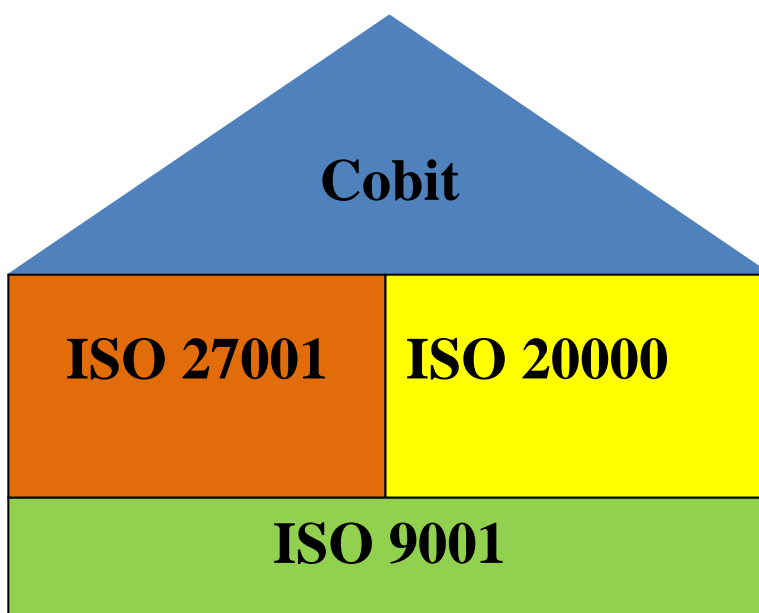


Figura 5 - Relacionamento entre governança de TI e Normas ISO de Sistemas de Gestão em TI

Conforme demonstrado no corpo do trabalho, os benefícios gerados por cada modelo adotado, distribuem-se em todas as áreas trazendo vantagens competitivas relativas as áreas: financeira, operacional e de relacionamento com clientes e fornecedores:

a) Área financeira:

- Utilização qualificada dos recursos humanos;

- A redução de custos é mais fácil de ser identificada, pois todos os processos são definidos e monitorados através de métricas bem definidas;
- Os processos de gerenciamento de incidentes e de problemas identificam e removem as causas das falhas nos serviços;
- As mudanças passam a ser planejadas e implementadas com segurança, há uma significativa redução em mudanças mal sucedidas;
- Os serviços são desenhados para atingir metas de qualidade, passam a ser considerados como um valor;
- Melhor gerenciamento de capacidade e conseqüentemente racionalização de custos;
- Há uma garantia de continuidade dos serviços e uma redução drástica nos prejuízos eventuais da interrupção dos mesmos;
- Redução dos prejuízos com a falta de segurança da informação;
- Melhor planejamento financeiro em relação à Infraestrutura e serviços de TI.

b) Área Operacional:

- O gerenciamento de processos faz com que a área operacional das organizações passe de ações predominantemente reativas para pró-ativas;
- Os controles de documentação, registros e qualidade tornam os processos mais confiáveis;
- Os números de incidentes são reduzidos e os remanescentes têm rápida resolução;
- Melhor gerenciamento do conhecimento;
- Melhor no gerenciamento de nível de serviço e carga de trabalho;
- Riscos na infra-estrutura e dependências são facilmente identificáveis;
- Redução na indisponibilidade dos Serviços Vitais para o Negócio;
- Gerenciamento adequado da segurança da informação.

c) Área de Recursos Humanos

- Regras e responsabilidades são claramente definidas e a equipe sabe o que será esperada dela;

- Qualificação da equipe de trabalho e melhoria das comunicações;
- Aumento da produtividade e maior foco nas prioridades do negócio;
- Aumento da motivação e satisfação no trabalho;
- Melhoria de forma geral na reputação da TI.

Além de todas estas vantagens, do ponto de vista comercial e institucional, uma empresa com certificações dá a seus clientes e fornecedores a segurança das negociações, uma vez que uma empresa com um sistema de gestão certificado indica que recebeu o aval de uma auditoria de terceira parte. Concluimos que a conformidade normativa e legal passará a ser exigência nas negociações internacionais, e os profissionais que atuam de acordo com estes sistemas de gestão conseqüentemente passam a ser mais valorizados.

REFERÊNCIAS

ABNT ISO/IEC 20000-1 , **Gerenciamento de serviços Parte 1: Especificação**;

ABNT ISO/IEC 20000-2 , **Gerenciamento de serviços Parte 2: Código de Prática**;

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito; **Gerenciamento de Serviços de TI na Prática** Uma abordagem com base na ITIL, Novatec, São Paulo 2007;

ABNT NBR ISO/IEC 27001:2006 - **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação** - Requisitos;

ABNT NBR ISO/IEC 27002:2005 - **Tecnologia da informação - Código de prática para a gestão da segurança da informação**;

BEAL, Adriana; **Segurança da Informação - Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações** - Editora Atlas - São Paulo 2005;

DIAS, Cláudia; **Segurança e Auditoria da Tecnologia da Informação** - Axcel Books do Brasil Editora - Rio de Janeiro 2005.

MELO, Carlos Henfrique Pereira Mello; **ISO 9001:2000 – Sistema de Gestão da Qualidade para Operações de Produção e Serviços**

PACHECO, Roberto C. S. e Tania Fátima Calvi Tait; **Tecnologia da informação: Evolução e Aplicações** - Teor. Evid. Econ., Passo Fundo, v. 8, n. 14, p. 97-113, maio 2000

SANTOS, Sandra Sergi; **A Governança de TI – Gestão de TI através de portfólios**; < www.gestaopm.com.br/documentos/GovTIcom_port_completo.pdf>

PRESSMAN, Roger S.; **Engenharia de Software – Mc Graw Hill AMGH Editora**

Ltda. São Paulo 2010.

TEIXEIRA, Cesar Aparecido; **Aspectos relevantes proeminentes das boas práticas da Governança Corporativa no cenário organizacional globalizado;**
<www.slideshare.net/rodrigo.afonseca/governana-corporaiva-no-cenrio-global-organizacional-edit-presentation>

PERES, João R; **O que é governança de TI**
<<http://www.profissionaisti.com.br/2009/03/o-que-e-governanca-de-ti/>>